

# Eine kurze Einführung

in die Thematik der multifunktionalen Kartensysteme  
Dr. Wolf-Rüdiger Voss, CashCard Automaten GmbH

Ganz einfach ist es nicht, sich im dichter werdenden Dschungel multifunktionaler Kartensysteme mit einer Vielzahl unterschiedlicher Anbieter und Techniken zurechtzufinden, zumindest dann nicht, wenn man sich nicht täglich mit diesem Thema beschäftigt und eigentlich doch nur schnell und ohne den Kostenrahmen zu sprengen zu einer einfachen und einheitlichen Lösung für eine Handvoll innerbetrieblicher Funktionen kommen möchte. Um Ihnen die Orientierung ein wenig zu erleichtern habe ich auf den folgenden Seiten zusammengefasst, was Sie über Kartensysteme wissen sollten und welche grundlegenden Gesichtspunkte bei einer Kaufentscheidung zu beachten sind.

Wir starten mit einem Rückblick auf die Entwicklung des Mitarbeiterausweises bis hin zum heutigen Stand der Technik. Dabei erfahren Sie, welche technischen Möglichkeiten es grundsätzlich gibt und welche wichtigen Kartentechnologien den Markt bestimmen. Danach werden wir zentrale Fragen bezüglich der Manipulationssicherheit und der Betriebssicherheit ansprechen. Mit diesem Grundwissen gerüstet wenden wir uns dann den multifunktionalen Mitarbeiterausweisen zu und diskutieren, welche Vorteile oder Nachteile bestimmte Systemkonstellationen haben und was grundsätzlich bei der Einführung eines solchen Systems beachtet werden muss. Schließlich stellen wir nochmals alle wichtigen Kriterien zusammen. Danach sollten Sie zumindest gegen schwerwiegende Fehlentscheidungen gewappnet zu sein.

## Wie alles angefangen hat ...

Alles fing ganz einfach an. Mit Lochkarten. Entsprechend dem Stand der Speichertechnik in der aufkommenden Computerindustrie Ende der 60er Jahre waren dies wohl die ersten Medien, die sinnvoll für innerbetriebliche Anwendungen wie Zutritt und Zeiterfassung einsetzbar waren. Nun noch die Pappe durch PVC ersetzen und obendrauf ein Polaroid kleben und der **multifunktionale Mitarbeiterausweis** war geboren. Schnell wurde klar, dass diese Technik einen entscheidenden Nachteil hat: die Informationen auf der Karte können nicht nachträglich geändert oder angepasst werden. Dies gilt gleichermaßen für einige andere Techniken, die in den folgenden Jahren auf den Markt kamen wie z.B. Infrarotausweise, Induktivausweise oder Barcodeausweise. Im Bereich der multifunktionalen Kartensysteme haben diese Datenträger heute kaum noch eine Bedeutung.

In den 70er Jahren wurde in der Computerindustrie die Speicherung von Daten auf Magnetband zum Standard. In einigen Bereichen entstand die Notwendigkeit, kleine Datenmengen in kompakter Form auf einem wiederverwendbaren Datenträger abzuspeichern. In diesem Zusammenhang entstand die Idee, ein kurzes Stück Magnetband auf eine feste Unterlage zu kleben und als flexiblen Datenträger zu verwenden. Auf einem solchen Medium konnte man nun z.B. kleine Programme für die ersten auf dem Markt erhältlichen programmierbaren Taschenrechner speichern. Die so entstandene **Magnetkarte** war gegenüber der Lochkarte schon recht fortschrittlich. Daten konnten, für das Auge unsichtbar, schnell gelesen und geschrieben werden. Funktionen wie z.B. die Speicherung eines Guthabens auf der Karte waren nun möglich.

In den folgenden Jahren setzten sich durch die große Verbreitung von Bankkarten auch im innerbetrieblichen Bereich **Karten im Kreditkartenformat** als Mitarbeiterausweis durch. Auf dem Weg zum multifunktionalen Ausweis hat die Kreditkarte zudem mit der Einführung der ISO-Codierung Maßstäbe gesetzt: der Standard-Magnetstreifen verfügt danach über 3 Magnetspuren, die für verschiedene und voneinander unabhängige Anwendungen genutzt werden können. Die anfänglich recht störanfälligen LoCo-Magnetstreifen wurden Mitte der 80er Jahre von einigen Herstellern durch HiCo-Magnetsreifen (hohe Koerzitivität) ersetzt, die nicht mehr durch Magneten, wie man sie z.B. in Lautsprecherboxen findet, abgelöscht werden konnten und damit, zusammen mit anderen Maßnahmen, die Karten recht robust machten. Zwischenzeitlich ist die Magnetkarte dennoch auf dem Rückzug, denn auch hier gibt es einige Nachteile, insbesondere die hohen Kosten für den Service an den Magnetkartenlesern und die geringe Kopiersicherheit der Karte.

## Die ersten Chips ...

In den 80er Jahren kam eine neue Technik auf, mit der Daten dauerhaft auf einem Chip gespeichert werden konnten. Wesentlich war dabei, dass die Daten auch dann erhalten blieben, wenn der Chip nicht mit Strom versorgt wurde. Unter Spannung konnte man die Daten dann beliebig lesen, schreiben und verändern. Auch diese Technik wurde für Karten nutzbar gemacht. Die **kontaktbehaftete Chipkarte** erreichte zunächst als Telefonkarte und später als Krankenversicherungskarte allgemeine Bekanntheit. Die Schreib-/Lesegeräte für die Chipkarte sind einfach aufgebaut und somit preiswert und wartungsfreundlich. Darüber hinaus wurde den Chips nach und nach eine gewisse Eigenintelligenz verpasst, so dass die Karteninformationen nicht mehr für jedermann lesbar oder gar kopierbar waren. Wichtig zu wissen ist hierbei, dass es nicht etwa nur eine Standard-Chipkarte gibt, sondern Duzende verschiedener Typen mit unterschiedlichen Eigenschaften.

Leider erwies sich auch die kontaktbehaftete Chipkarte nicht als perfekte Lösung. Probleme ergeben sich insbesondere dann, wenn die **Kartenkontakte verschmutzt** sind oder die Karte im Bereich des Chips geknickt wird. Defekte Chips können mit einfachen technischen Mitteln nicht mehr ausgelesen werden. Zudem sind die Kartenleser nicht 100% wartungsfrei, da der **Mechanismus für die Kontaktierung** des Kartenchips exakt arbeiten muss und einer hohen Beanspruchung ausgesetzt ist. Auch der geringe technische Aufwand, der erforderlich ist, um Chipkarten zu programmieren, stellt ein gewissen Problem dar, denn dies hat zur Folge, dass Heerschaaren unterschiedlich motivierter Hacker kontinuierlich versuchen, weit verbreitete Chips zu knacken und trotz der Sicherheitsmechanismen zu kopieren. Um dennoch eine gewisse Sicherheit zu gewähren, werden **Chipkarten oft proprietär** eingesetzt, was aber andererseits bedeutet, dass Anwendungen anderer Hersteller nicht auf dem selben Chip realisiert werden können. Es handelt sich somit um Insellösungen mit allen üblichen Vorteilen und Nachteilen.

Das Problem der Insellösung kann prinzipiell mit sogenannten **SmartCards** (schlaue Karten) gelöst werden. Hierbei handelt es sich um hochentwickelte Chipkarten mit Mikroprozessor und eigenem Betriebssystem. Im Prinzip kann man eine SmartCard als einen kleinen Computer betrachten. Mehrere verschiedene Anwendungen können unabhängig voneinander aufgebracht werden. Leider gibt es noch keinen einheitlichen Standard und die Karten sind für die Anwendungen, um die es hier geht, unverhältnismäßig teuer und aufgrund der hohen Komplexität teilweise auch zu langsam. Ein Einsatz als multifunktionaler Mitarbeiterausweis erscheint mir derzeit nicht ratsam, es ist ein wenig, als würde man mit Kanonen auf Spatzen schießen.

## Kontaktlos in die Zukunft ?

Die Antwort auf viele der Probleme mit kontaktbehafteten Chipkarten ist die in den 90er Jahre entwickelte **kontaktlose Chipkarte**, heute auch häufig mit dem Modewort **RFID (Radio Frequency Identification)** bezeichnet. Auch diese Karten verfügen über einen Kartenchip, allerdings liegt dieser geschützt im Inneren der Karte und ist von außen nicht sichtbar. Die Kommunikation mit der Karte erfolgt über eine ebenfalls innerhalb der Karte liegende Antenne. Wenn die Karte in den Sendebereich eines Kartenlesers gehalten wird, empfängt die Karte über die integrierte Antenne ein starkes Signal. Dieses Signal enthält die zu übertragenden Informationen und versorgt (und das ist das eigentlich geniale an dieser Technik) gleichzeitig den Kartenchip mit Strom.

Insgesamt ist die Technik für kontaktlose Chipkarten zwar aufwändiger und teurer als die kontaktbehaftete Version, dafür aber zu **100% wartungsfrei** und wesentlich robuster. Auch der Sicherheitslevel ist um einiges höher. Die übertragenen Daten sind in der Regel verschlüsselt und können nicht mit einfachen Mitteln demoduliert oder entschlüsselt werden. Einige Hersteller wie z.B. LEGIC stellen durch ein ausgeklügeltes Lizenzierungssystem sicher, dass Karten und Lesegeräte über einen gemeinsamen Lizenzschlüssel verfügen müssen, um miteinander kommunizieren zu können. Für Dritte, die nicht über einen solchen Lizenzschlüssel und über die entsprechenden Informationen verfügen, ist eine Manipulation oder ein Kopieren der Daten nicht möglich. Darüber hinaus können auf kontaktlosen Karten wie **LEGIC** oder **Mifare** standardmäßig mehrere Anwendungen gleichzeitig und unabhängig voneinander realisiert werden. Die kontaktlose Chipkarte ist somit die **derzeit beste Wahl** für einen zeitgemäßen, sicheren und multifunktionalen Werksausweis, zumal auch die Preise für Karten und Leser in den letzten Jahren nach und nach in einem vernünftigen Bereich angelangt sind.

Die zukünftige Entwicklung geht in Richtung **kontaktlose SmartCard**, wobei hier noch kein einheitlicher Standard erkennbar ist. Mehr als heute wird das Preis-/Leistungsverhältnis abzuwägen sein, da von der Komplexität der neuen Kartenchips meist nur ein Bruchteil wirklich benötigt wird.

Sie haben nun einiges über die verschiedenen Kartentypen erfahren, die für ein innerbetriebliches Kartensystem eingesetzt werden können. Auf der folgenden Seite erfahren Sie, welche Sicherheitsaspekte zu beachten sind, wenn Sie ein Kartensystem für Ihren Betrieb planen.

# Sicher ist nicht gleich sicher

Ein wichtiger Sicherheitsaspekt eines Kartensystems ist der Schutz der Datenträger vor Manipulationen. Der **Manipulationsschutz** wird bei kontaktlosen und kontaktbehafteten Chipkarten meist dadurch realisiert, dass zum Lesen und Beschreiben der Karte spezielle Schlüssel benötigt werden. Es handelt sich dabei um Kombinationen von Zahlen und Buchstaben die entweder zufällig erzeugt werden oder vom Anwender selbst festgelegt werden können. Die verschiedenen Techniken unterscheiden sich darin, wie lang diese Schlüssel sind, wie viele davon es gibt, wie die Schlüssel anzuwenden sind und wie die Schlüssel zwischen Leser und Karte übertragen werden.

Einfache kontaktbehaftete Chipkarten wie die **SLE4442** arbeiten mit einem **Schlüsselcode** der vom Leser gesendet werden muss, wenn man die Karte beschriften möchte. Wird dieser Code 3 mal hintereinander falsch präsentiert, sperrt sich die Karte dauerhaft selbst. Gegenüber der Lochkarte und der Magnetkarte ist dies natürlich ein gewaltiger Fortschritt. Ganz sicher ist diese Technik leider nicht. Mit entsprechenden Vorrichtungen kann der Code während der Übertragung abgehört werden und somit ist eine Manipulation von Karten möglich. Systeme, die sich allein auf solche allgemein zugänglichen Konzepte verlassen, wurden in der Vergangenheit schon mehrfach ohne allzu großen technischen Aufwand geknackt.

Bei komplexeren kontaktbehafteten und kontaktlosen Karten (z.B. **LEGIC**) kommen aufwändige **Verschlüsselungsmechanismen** und, im Falle LEGIC, ein komplexes Lizenzierungssystem zum Einsatz. Insgesamt erhöht sich dadurch die Sicherheit beträchtlich. Darauf näher einzugehen würde hier zu weit führen. Rein rechnerisch sind Verschlüsselungsverfahren wie Triple-DES nicht oder nur mit sehr großem technischen Aufwand zu knacken. Angriffe auf diese Systeme erfolgen eher durch die Hintertür und basieren meist auf Nachlässigkeiten in den Bereichen, wo die Schlüssel und die Sicherheitsinformationen verwaltet werden oder auf groben Sicherheitslücken in der Software, wenn beispielsweise ein Programmierer vergessen hat, die Verschlüsselung zu aktivieren.

CashCard und andere professionelle Systeme wenden zusätzlich eigene Verschlüsselungsverfahren und weitere Techniken an, um die Kopiersicherheit, Manipulationsicherheit und Zuverlässigkeit der Karten weiter zu erhöhen. Dass über diese Verfahren im Detail keine Auskunft gegeben wird versteht sich natürlich von selbst und ist ebenfalls ein wichtiger Bestandteil des Sicherheitskonzeptes.

# Thema Betriebssicherheit

In der Praxis ist die **Betriebssicherheit** des Kartensystems von noch größerer Bedeutung als die Manipulationssicherheit. Hier gibt es deutliche Unterschiede zwischen den angebotenen Systemen. Für einen Laien sind die technischen Unterschiede in der Regel nicht ohne weiteres erkennbar. Man kommt der Sache aber schon näher, wenn man einige allgemeine Kriterien betrachtet. Stellen Sie sich bitte die folgenden Fragen:

- Wie lange ist das System bereits auf dem Markt ?
- Wird das System regelmäßig überarbeitet ?
- Was berichten Anwender, die bereits mit dem System arbeiten ?
- Gibt es einen guten vor Ort Service, Hotline, Serviceverträge ?
- Welche Referenzen kann der Anbieter vorweisen ?
- Wie weit deckt bereits die Standardausführung den Bedarf ab ?
- Wie kompetent ist die Beratung durch den Lieferanten ?

Fallen die Antworten auf diese Fragen positiv aus, so haben Sie schon eine gewisse Garantie dafür, dass die Betriebssicherheit des Systems gewährleistet ist. Darüber hinaus sollten Sie sich mit folgenden Überlegungen auseinandersetzen:

1. Werden Daten wie Kartenguthaben und Kartensperrungen zentral auf einem Server hinterlegt, dann müssen alle Endgeräte ständig Online sein. Wenn das Netzwerk oder der Server ausfällt, kommt das System zum Stillstand. Es ist daher von großem Vorteil, wenn die individuellen Daten wie das Kartenguthaben auf der Karte selbst hinterlegt sind und wenn jedes Endgerät über alle wichtigen Systemdaten verfügt. Nur so ist ein sicherer Offline-Betrieb möglich.

2. Insgesamt kommt den Möglichkeiten der Vernetzung und der Verfahrensweise in Fällen, wo eine Vernetzung nicht möglich ist, eine große Bedeutung zu. Auch die Frage, wie sicher die in den Endgeräten gespeicherten Vorgangsdaten im Falle eines Stromausfalls oder Netzwerkausfalles sind, ist nicht zu vernachlässigen.

3. Erfahrungsgemäß treten, abgesehen von Netzwerkproblemen, die allermeisten Betriebsstörungen an Verkaufsautomaten auf. Hier gibt es eine große Vielfalt an Typen und Schnittstellen die nicht von allen Herstellern gleichermaßen gut unterstützt werden. Sie sollten genau prüfen, ob Ihre bestehenden oder die neu anzuschaffenden Automaten zu dem gewünschten Kartensystem kompatibel sind.

# Multifunktionalität hat ihren Preis

**Die Multifunktionalität des Mitarbeiterausweises wird bisher meist dadurch erreicht, dass die einzelnen Spuren auf dem Magnetstreifen, bestimmte Speicherabschnitte auf dem Kartenchip oder die Segmente auf einer kontaktlosen Karte für die unterschiedlichen Anwendungen und Systemlieferanten entsprechend aufgeteilt werden. Obwohl dies in der Praxis meist problemlos funktioniert, sollte man zwei Gesichtspunkte nicht übersehen:**

1. Wenn die Bereiche auf der Karte nicht konsequent gegeneinander abgeschottet und durch die Eigenintelligenz der Karte geschützt sind, besteht die Gefahr, dass die Anwendungen sich gegenseitig beeinflussen, insbesondere dass Daten unbeabsichtigt modifiziert oder gelöscht werden. Die Ursache des Fehlers lässt sich in solchen Fällen nur sehr schwer feststellen, zumal jeder Hersteller dazu neigt, für das Problem die anderen Anwendungen verantwortlich zu machen. Ein Paradebeispiel wäre z.B. ein defekter Magnetkopf, der beim Schreiben seiner Magnetspur die Daten auf der benachbarten Spur beschädigt.

2. Die unterschiedlichen Segmente oder Spuren auf der Karte müssen in der Regel für jede Anwendung einzeln vorbereitet (initialisiert) werden. Dabei kennzeichnet die jeweilige Anwendung ihr zugeordnetes Segment und stellt eventuell durch Verschlüsselung und zusätzliche Verfahren sicher, dass die Segmentdaten nicht von anderen Anwendungen gelesen oder verändert werden können. Dies führt in der Praxis zu einem erheblichen Verwaltungsoverhead bei der Vorbereitung der Karten. Oft müssen die Karten von Hersteller zu Hersteller geschickt werden oder es müssen geheime Informationen und Initialisierungsmedien zwischen Unternehmen ausgetauscht werden, die eigentlich im Wettbewerb zueinander stehen. Am Ende sieht sich der Kunde oft gezwungen, für jedes System eine eigene Codierstation anzuschaffen, wobei der Personalstamm und die Kartendaten für jedes System separat mit unterschiedlicher Software verwaltet werden müssen.

**Die Multifunktionalität bezahlt man also in der Regel mit gewissen Einschränkungen bei der Sicherheit und mit einem hohen Aufwand für die Abstimmung zwischen den beteiligten Systemlieferanten.**

# Auswege aus dem Chaos

**Multifunktionalität ist also, wie wir gesehen haben, nicht umsonst zu haben und stets mit einem hohen Aufwand bei der Planung und bei der Verwaltung des Systems verbunden. Aus diesem Dilemma gibt es jedoch Auswege:**

1. Man sucht sich einen Lieferanten, der alle benötigten Komponenten aus einer Hand liefert. Sofern der Lieferant auch Hersteller der gelieferten Produkte ist, sollte man davon ausgehen können, dass alle Komponenten perfekt zusammenarbeiten. Problematisch ist dabei, dass es zum einen nicht allzu viele Anbieter mit einem breiten Produktspektrum auf dem Markt gibt, zum anderen macht man sich natürlich von dem gewählten Anbieter abhängig.

2. Man entscheidet sich für eine sichere Kartentechnologie, die von einer großen Anzahl von Anbietern unterstützt wird, die sich untereinander absprechen und in Verbindung stehen. Im deutschsprachigen Raum trifft dies derzeit eigentlich nur für die kontaktlose LEGIC-Technologie zu. Das entsprechende Partner-Netzwerk finden Sie im Internet unter **[www.legic.com](http://www.legic.com)** .

3. Man entscheidet sich für eine offene segmentierte Kartentechnologie die gut dokumentiert ist und deren technische Details allen Systementwicklern frei zugänglich sind und nimmt dabei eine etwas geringere Sicherheit in Kauf. Man beachtet weiterhin, dass es sich nicht um eine exotische Technologie handelt, sondern um eine, die bereits in großem Maßstab eingesetzt wird. In diesem Fall käme die Mifare Karte in Betracht.

**Idealerweise sollte unter Berücksichtigung aller genannten Punkte das gewünschte Kartensystem auf Basis von LEGIC oder Mifare aus einer Hand geliefert werden. Sollte sich später herausstellen, dass der Lieferant bestimmte Teilbereiche nicht gut abdecken kann, hat man jederzeit die Möglichkeit, auf Produkte eines anderen Herstellers auszuweichen. Sie umgehen somit elegant die Abhängigkeit von einem einzigen Anbieter ohne auf die Vorteile der Lieferung aus einer Hand zu verzichten.**

# Interoperabilität ist nicht selbstverständlich

**Vielen Anwendern bereitet es grundsätzlich Probleme zu verstehen, warum die Daten, die eine bestimmte Anwendung auf die multifunktionale Karte aufbringt, nicht auch von allen anderen Anwendungen verwendet werden können.**

Wenn z.B. der Kantinenbetreiber ein anderes System installiert als der Automatenbetreiber, dann kann das in der Kantine aufgewertete Guthaben nicht an den Automaten verbraucht werden. Oder wenn eine Karte im Zutrittsbereich über die Zutrittssoftware gesperrt wird, funktioniert die Karte weiterhin in der Kantine und an den Automaten. Oder wenn Sie einen Aufwerter für das Kantinensystem benötigen, kann dieses Gerät nur beim Hersteller des Kantinensystems bezogen werden. Mit den Geräten von Fremdherstellern funktioniert es nicht.

**Warum ist das eigentlich so?** Wie bereits gesagt, schreibt jeder Hersteller seine eigenen Daten in ein eigenes Segment oder auf eine eigene Spur der Karte. Meist werden die Daten zusätzlich verschlüsselt. Da es schon aus Sicherheitsgründen keinen einheitlichen Standard für die Daten auf der Karte gibt, kann jede Anwendung nur die eigenen Daten lesen und schreiben.

**Eine echte Interoperabilität wäre nur dann möglich, wenn sich verschiedene Hersteller genau untereinander abstimmen würden und ihre Software entsprechend anpassen. Solche Lösungen gibt es auf dem Markt nur wenige und sie sind in ihrer Funktionalität meist sehr beschränkt. Auch hier ist ein System aus einer Hand, das auf einer einheitlichen Plattform basiert, von Vorteil. Die angesprochenen Probleme gibt es dabei naturgemäß nicht.**

Nachdem Sie nun, ohne Anspruch auf Vollständigkeit, die wesentlichen Gesichtspunkte im Zusammenhang mit der multifunktionalen Karte betrachtet haben, finden Sie auf der folgenden Seite eine Zusammenfassung aller aus meiner Sicht für eine Kaufentscheidung wesentlichen Aspekte.

# Jetzt haben Sie die Übersicht

## Welche Karte ist die richtige ?

- wenn das System preiswert sein soll und proprietär sein darf, dann Chipkarte
- wenn Sicherheit und Verfügbarkeit wesentlich sind, nehmen Sie LEGIC
- wenn einfache Handhabung und offene Struktur wichtiger sind, dann Mifare

## Welche Funktionsbereiche müssen berücksichtigt werden ?

- Kartenpersonalisierung (Daten verwalten, Karten codieren, Karten drucken)
- Zutrittskontrolle (Leser für Innenbereich und Außenbereich)
- Zeiterfassung (Möglichkeit zur Anbindung an Lohnbuchhaltung)
- Kantinenabrechnung (eventuell Cafeteria, Mitarbeitershops, Vesperwagen)
- Zwischenverpflegung (Heißgetränke, Kaltgetränke, Snacks, Süßwaren)
- Parkraumbewirtschaftung für Mitarbeiterparkplatz und Kundenparkplätze

## Welche Fragen sollte man stellen ?

- welcher Aufwand entsteht für die Pflege des Gesamtsystems ?
- wer garantiert, dass alle Systemkomponenten problemlos zusammenarbeiten ?
- kann das System auch nachträglich jederzeit ausgebaut werden ?
- ist der Betriebsrat im Bilde und unterstützt er die Einführung des Systems ?
- gibt es Anwender, die Auskunft über das System geben können ?
- können bestehende Komponenten wie Automaten eingebunden werden ?
- können Datenbanken wie der Mitarbeiterstamm problemlos importiert werden ?
- können alle Komponenten auch bei einem Netzwerkausfall weiterarbeiten ?

## Nach welchen Kriterien sollte man sich entscheiden ?

- wählen Sie Lieferanten, die viele Komponenten aus einer Hand liefern
- wählen Sie Komponenten, die auf einer gemeinsamen Plattform basieren
- wählen Sie Lieferanten mit einem guten vor Ort und Hotline Service
- wählen Sie einen Lieferanten mit Sachkompetenz, lassen Sie sich beraten
- wählen Sie Hersteller, die schon länger auf dem Markt sind
- wählen Sie Systeme, die kontinuierlich weiterentwickelt werden