Sicherung von Chipkarten

Lars Morres

Humboldt-Oberschule

Kurs: Informatik Inf-02

Juni 2002

Inhaltsverzeichnis

1. Allgemeines zur Chipkarte

Der Zahlungsverkehr hat sich, vor allem in dem privaten Bereich, stark verändert

Früher waren die üblichen Zahlungsmittel hauptsächlich Bargeld und Schecks, heute hingegen wird immer häufiger die Kredit- bzw. Chipkarte zum Zahlungsmittel.

Seit den Neunziger Jahren setzt sich die Chipkarte in immer weiteren Bereichen des öffentlichen Lebens durch. Relative Verbreitung fand die Chipkarte in den Bereichen des Zahlungsverkehrs, der Datenspeicherung und der Zugangskontrolle. Im Zahlungsverkehr beispielsweise wird sie in Form der so genannten Geldkarte eingesetzt, in der Datenspeicherung ist nahezu jeder mit der Chipkarte in Form seiner Krankenkarte in Berührung gekommen und inzwischen wird sie an einer Vielzahl von Universitäten zur Zugangs- bzw. Anwesenheitskontrolle an die Studenten ausgegeben.

Die Chipkarte ist eine Plastikkarte mit einem eingebauten Mikroprozessor, der aktiviert wird, wenn die Chipkarte in einen passenden Automaten eingeführt wird. Je nach Anwendungsgebiet kann der Prozessor für die jeweiligen Anforderungen programmiert werden. Mit der Nutzung von Chipkarten ergaben sich nicht nur große Vorteile, sondern auch Risiken.

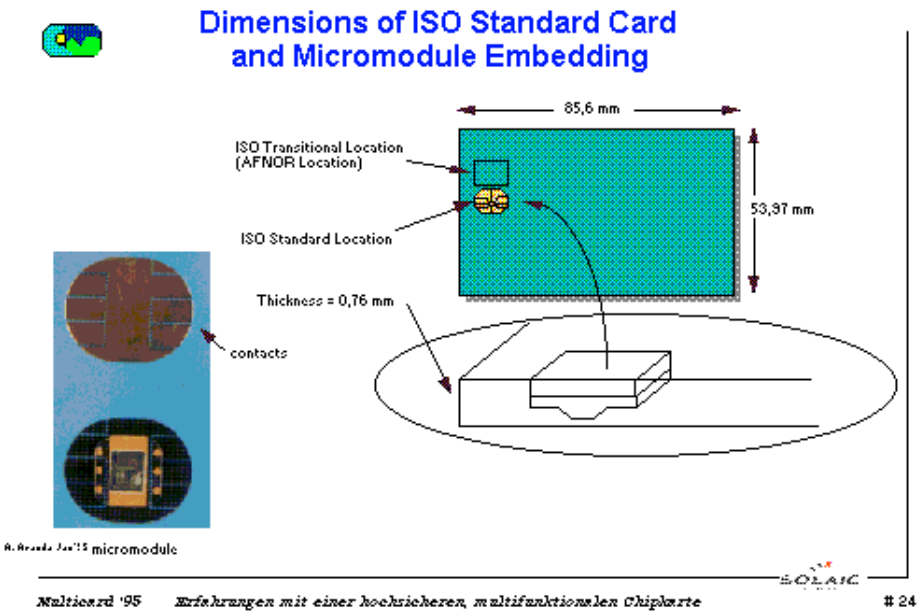
Die Vorteile für den Chipkartenbesitzer liegen zum Beispiel in den verkürzten Wartezeiten beim Geldabheben und der ständigen Verfügbarkeit als Zahlungsmittel, der einfacheren und praktischeren Handhabung in Krankheitsfällen. Die Ausgabe von Chipkarten ist für die verschiedenen Institutionen nicht ganz uneigennützig - sie würden sie nicht verwenden, wenn sie nicht ihre eigenen Vorteile als wesentlichen Antrieb erkannt hätten. Zum einen lassen sich durch Rationalisierung im Personalbereich erhebliche finanzielle Einsparungen erreichen, zum anderen ermöglicht eine Chipkarte auch die Bindung von Kunden an die Institution. Außerdem können diese Institutionen Vorgänge schneller und fehlerfreier durchführen und wesentlich mehr Informationen über ihre Kunden erfahren.

Risiken sind in zwei sensiblen Bereichen von besonderer Bedeutung. Einer dieser Bereiche ist die Datenübertragung bei der, wenn Fehler auftreten und die Chipkarte somit ihre Funktion nicht erfüllt, es zu erheblichen Wertverlusten und dadurch logischerweise zu Unzufriedenheit und Vertrauensverlust des Besitzers führen könnte. Der andere Aspekt, der Risiken mit sich bringt, ist die unbefugte Nutzung der Karte. Wenn diese Karte an einen Dritten gerät muss gesichert sein, dass dieser mit der Chipkarte nichts anfangen kann.

2. Aufbau einer Chipkarte

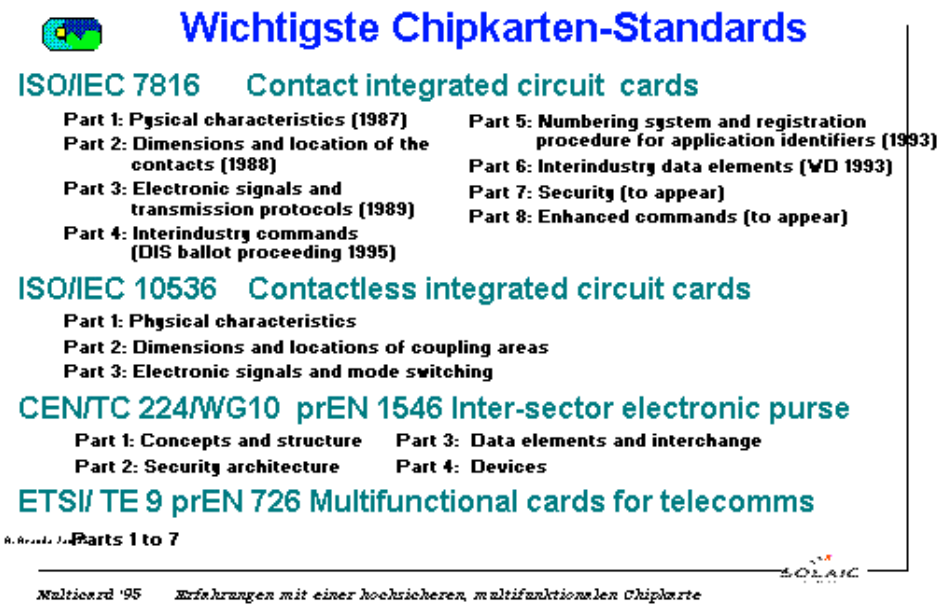
2.1. Größe einer Chipkarte

Die Größe einer Chipkarte ist in der ISO/IEC 7816 festgelegt.



2.2. Normen

Die wichtigsten Normen zum Aufbau einer Chipkarte sind in folgender Abbildung dargestellt:



2.3. Arten von Chipkarten

2.3.1. Speicherchipkarten

Speicherchipkarten können elektrisch programmiert und codiert werden. Sie behalten ihren Speicherinhalt, auch nach Abschalten des Stroms bzw. bei dem Herausnehmen der Karte aus einem Automaten, bei. Ein bereits codierter Speicher kann ausschließlich mit Hilfe von ultravioletten Strahlen neu programmiert werden. Die Größe eines durchschnittlichen Speicherchips beträgt ca. $1mm^2$.

2.3.2. Mikroprozessorkarten

Mikroprozessorkarten beinhalten Mikroprozessoren, die praktisch wie normale Rechner aufgebaut sind, genannt Central Processing Unit (CPU). Sie verfügen über einen zentralen Rechner und verschiedene Speicherarten. Diese so genannten CPUs können die zu speichernden Daten nach jeweils programmierten Regeln berechnen und kontrollieren. Sie haben natürlich eine wesentlich größere Funktionsbreite und eine höhere Sicherheit gegenüber Manipulation als Speicherchipkarten.

2.3.3. Kryptoprozessorkarten

Kryptoprozessorkarten sind Mikroprozessorkarten, die über einen zusätzlichen Prozessor verfügen. Da die Sicherheitsanforderungen für Chipkarten sehr hoch sind, wurde es notwendig mindestens einen weiteren Prozessor ausschließlich zur Verschlüsselung von Daten in den Chip zu integrieren.

3. Möglichkeiten der Sicherung

Um die in Kapitel 1 angesprochenen Risiken der Chipkartennutzung zu vermeiden, gäbe es verschiedene Möglichkeiten:

3.1. Funktionsbreite und Speicherinhalt

3.1.1. Verringerung der Funktionsbreite

Eine Variante wäre, wichtige und sensible Daten bzw. Informationen nicht auf den Chipkarten zu speichern. Da hierbei aber der Nutzen der Chipkarte stark eingeschränkt wäre, wären weder Vorteile auf Seiten der Besitzer, noch auf Seiten der ausgebenden Stellen zu verzeichnen. Diese Handhabung der Sicherung von Chipkarten ist nur eine theoretische Überlegung, die der Vollständigkeit halber hier erwähnt wird.

3.1.2. Erhaltung der Funktionsbreite

Würden jedoch wichtige Informationen gespeichert werden, müsste jeder Besitzer auf seine persönliche Chipkarte Acht geben. Da diese Möglichkeit den Besitzern verständlicherweise zu risikoreich wäre, müssten technische Maßnahmen getroffen werden, die unabhängig von den Benutzern wirken.

3.2. Technische Maßnahmen zur Sicherung

Um eine Risikominderung bei gleicher Funktionsbreite von Chipkarten zu erhalten, müsste ein geeignetes System zur Sicherung von Chipkarten entwickelt werden. Die Grundlage solch einen Systems ist eine Form der Verschlüsselung.

Um Geld an einem Automaten abzuheben, wird nicht nur eine Kreditkarte benötigt, sondern auch eine dazugehörige Geheimzahl, genannt PIN (Personal Identification Number). Diese PIN ist selbstverständlich nicht auf dieser Kreditkarte gespeichert und auch nicht im Geldautomaten oder in einem Bankcomputer, da, wenn die Karte in falsche

Hände geraten würde, unbefugt Geschäfte getätigt werden könnten. Dadurch wird beispielsweise auch ausgeschlossen, dass ein Bankangestellter, der Zugriff zu dem Bankcomputer hat, durch Kenntnis der PIN Zugriff auf das zugehörige Konto erhält.

Der Bankcomputer erkennt anhand eines bestimmten Schlüssels, die Zugehörigkeit der PIN zu dem Bankkonto. Es gibt nun sehr verschiedene Möglichkeiten eine Zahlenfolge zu verschlüsseln. Grob lassen sich Verschlüsselungsverfahren in folgende Gruppen einteilen:

3.2.1. Verschlüsselung mit einfachen Funktionen

Bei einer Verschlüsselung mit einfachen Funktionen wird eine Geheimzahl mit einer beliebigen, festgelegten und geheim gehaltenen Funktion verrechnet. Hierbei hat man bei Kenntnis der geheimen Funktion die Möglichkeit die Verschlüsselung rückgängig zu machen. Das bedeutet, dass es keine absolute Sicherheit gibt die Geheimzahl vor der Entschlüsselung zu schützen.

Ein sehr einfaches Verfahren um eine Geheimnummer zu verschlüsseln ist das Additionsverfahren. Bei diesem Verfahren wird die zu verschlüsselnde Geheimzahl mit einer bestimmten Schlüsselzahl addiert bzw. subtrahiert. Um die Geheimzahl zu verschlüsseln wird diese mit einer Schlüsselzahl addiert, dies geschieht jedoch ohne Übertragung der Zehner. Das heißt, dass beispielsweise aus der Geheimzahl 6830 durch die Schlüsselzahl 2957, die verschlüsselte Geheimzahl 8787 entsteht. Andersherum wird bei dem Entschlüsseln die verschlüsselte Zahl mit der Schlüsselzahl subtrahiert. Dies wird wiederum ohne Übertragung der Zehner durchgeführt. Man erhält eine verschlüsselte Geheimzahl, die sich durch Kenntnis der Schlüsselzahl immer wieder leicht entschlüsseln lässt. Dies könnte zum Verschlüsseln der privaten Geheimnummer gebraucht werden, aber in öffentlichen Banken werden selbstverständlich komplexere Verschlüsselungsverfahren angewandt.

3.2.2. Verschlüsselung mit Einwegfunktionen

Um das Risiko der einfachen Entschlüsselung auszuschließen, wurde die Verschlüsselung mit Hilfe von Einwegfunktionen entwickelt. Die Einwegfunktionen haben die Eigenschaft, dass Informationen nicht mit den gleichen Schlüsseln entschlüsselt werden können, mit denen sie verschlüsselt wurden. In der Regel werden zur Verschlüsselung und Entschlüsselung von Informationen mittels Einwegfunktionen drei Schlüssel benötigt: zwei private und ein öffentlicher Schlüssel.

Mit Hilfe des einen privaten und des öffentlichen Schlüssels wird die Information codiert. Um sie wieder zu decodieren, wird der zweite private Schlüssel, in Verbindung mit dem öffentlichen Schlüssel, benötigt.

Die Prüfung der Legitimation in Verbindung mit Chipkarten ist ein sicherheitstechnisch sehr sensibler Bereich für den Codierungen nach dem Einwegverfahren zum Einsatz kommen.

Diese Sicherheitsprüfung bei Verwendung von Chipkarten ist folgendermaßen aufgebaut: Bei Ausgabe der Chipkarte teilt der Bankcomputer dem Kontoinhaber seine Geheimnummer zu, verschlüsselt die so genannte Klartext-PIN mit dem öffentlichen Schlüssel N und dem privaten Schlüssel E zu einer Geheimtext-PIN und speichert sowohl Geheimtext-PIN, als auch die Schlüssel N und E auf dem Chip der Karte. Steckt der Kontoinhaber die Chipkarte in den Geldautomaten, so wird er aufgefordert die Klartext-PIN einzugeben. Im Geldautomaten wird die Klartext-PIN mit den Schlüsseln N und E verschlüsselt und das Ergebnis mit der ebenfalls auf der Karte abgespeicherten Geheimtext-PIN verglichen. Stimmen diese Zahlen überein, so ist die Legitimation des Kontoinhabers für die Nutzung der Karte bestätigt. Daraufhin erfolgt im Bankcomputer eine Überprüfung der Zuordnung der Karte zu einem bestimmten Konto (mit Legitimation der Karte gegenüber der Bank). Dazu sendet der Bankcomputer eine Zufallszahl an die Karte. Im Chip der Karte wird mit den Schlüsseln N und E verschlüsselt. Gleichzeitig wird im Bank-

computer diese Zufallszahl ebenfalls mit den Schlüsseln N und E verschlüsselt. Stimmen diese verschlüsselten Zufallszahlen überein, so ist die Legitimation des Kunden zur Nutzung des entsprechenden Kontos gewährleistet.

4. Ausblick

Vor ca. zwei Jahrzehnten kamen die ersten Chipkarten in Frankreich und Deutschland auf den Markt. Mittlerweile sind es weltweit etwa 2 Milliarden Chipkarten, die im Umlauf sind. Die Entwicklung, die die Chipkarten in den letzen Jahrzehnten genommen haben, ist enorm. Jedoch ist die Entwicklung noch nicht abgeschlossen. In Zukunft werden Multifunktionschipkarten immer breiteren Stellenwert einnehmen. Neben ihrer Fähigkeit, in Sekundenbruchteilen mittels des sicher gespeicherten Schlüssels Datensätze zu ver- und entschlüsseln, sind sie schon bald echte Multi- Applikations- und Multi-Tasking-Computer. Zukünftige Chipkartencontroller-Generationen werden über eine hardwarebasierte „Memory Management Unit“ zur Separierung von Anwendungen verfügen. Mittels dieser Memory Management Unit können einzelne Applikationen sicher voneinander getrennt verwaltet werden und damit ohne gegenseitige Beeinflussung vollkommen unabhängig nebeneinander arbeiten. Somit wird es möglich, beispielsweise Banking-Applikationen, Zugangskontroll-Funktionen, Theater- oder Flugtickets und vieles mehr entsprechend den Wünschen des Benutzers auf eine Karte zu laden. So werden auf einer Karte, und weitere Anwendungen realisiert.

5. Literaturverzeichnis

[1] Rudolf Kippenhahn, Verschlüsselte Botschaften, rororo Sachbuch 60807, 2. Auflage Juni 2001

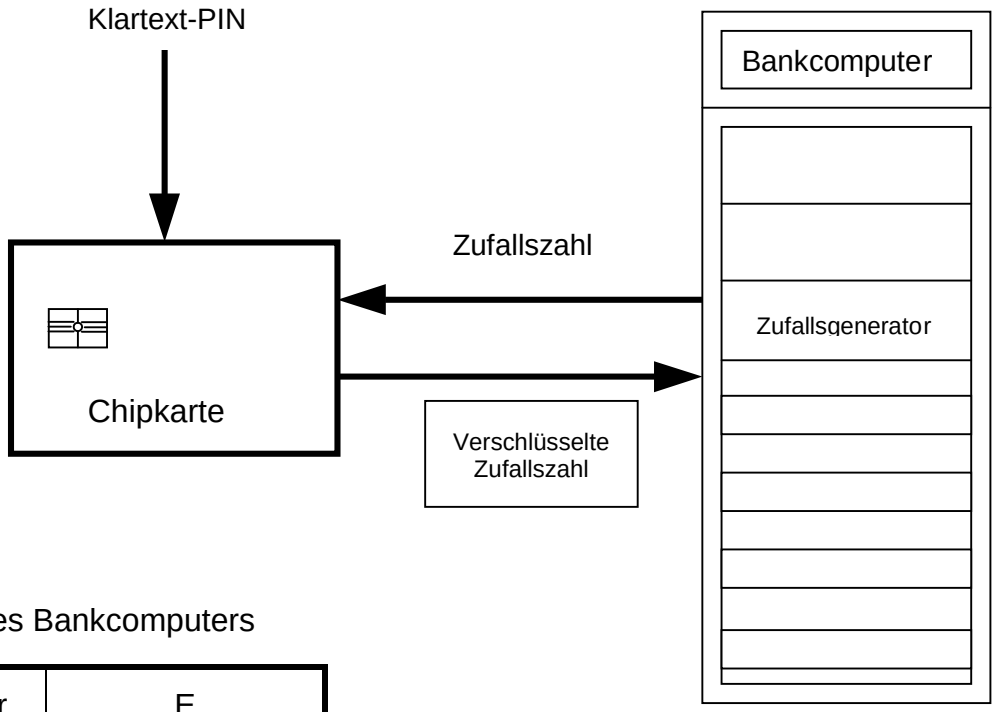
[2] Yahya Haghiri, Thomas Tarantino, Vom Plastik zur Chipkarte – Das Handbuch zur Herstellung von Chipkarten, Oktober 1999

[3] A. Aranda, SOLAIC Smart Cards, Groupe SLIGOS, Frankfurt/Main

[4] Ulrich Hamann, Leiter des Geschäftsbereichs Sicherheits- und Chipkarten-ICs, „Mit der Chipkarte in die digitale Welt“, Infineon Technologies AG, München

6. Anhang

Schematische Darstellung der Sicherheitsprüfung einer Chipkarte:



Speicher des Bankcomputers

Kontonummer	E
0254939	821893425
7673923	158762354
7475092	185782526
4537597	243469647
5782364	321995787
7723540	562123450
2765489	207378901
8975642	665560513
7976982	256987264
1050981	157126389
0566004	691344864
0654349	584813276