LANDIS & GYR

Plastikkarten – wie intelligent ist sicher?

A. S. Glass und J. L. Massey
Sonderdruck aus den Landis & Gyr-Mitteilungen 2/85

Plastikkarten – wie intelligent ist sicher?

A. S. Glass* und J. L. Massey**

Die zukünftige Rolle der Plastikkarte als Zahlungsmittel steht heute im Mittelpunkt weitreichender interdisziplinärer Diskussionen, die Spezialisten aus verschiedensten Kreisen beschäftigen und sowohl Bankfachleute und Elektrotechniker wie auch Sicherheitsspezialisten und Kriminalbeamte interessieren.
Im ersten Teil dieses Aufsatzes wird die allgemeine Problematik der Kartensysteme mit maschinell lesbaren Karten für Zahlungs- bzw. Zutrittszwecke umrissen und deren Anforderungen vor allem vom Standpunkt der Sicherheit aus betrachtet. Der zweite Teil befasst sich im wesentlichen mit den Fragen, in wieweit die Sicherheit durch kryptographische Methoden gewährleistet werden kann, und für welche Anwendungen elektronische Karten tatsächlich geeignet sind.
Es wird darauf eingegangen, welche Vor- und Nachteile intelligente, mit Mikroprozessor versehene Karten gegenüber konventionelleren Karten aufweisen. Es wird gezeigt, dass die Mikroprozessorkarte Möglichkeiten beinhaltet, die für mehrere Anwendungen hinreichende Sicherheit anbieten, und dass sie vor allem für Verwendung bei Onlinesystemen geeignet ist. Insbesondere bleibt noch etwas Spielraum für weitere Entwicklungen der Karte, falls vollständige Sicherheit für Onlinesysteme mit ungesicherten Terminals gefordert wird.
Ferner wird auch gezeigt, dass der höhere Preis heutiger ,,aktiver" Mikroprozessorkarten bei weitem nicht überall gerechtfertigt ist, weil die gleiche Sicherheit sich wirtschaftlicher mit etablierten, sicheren ,,passiven" Karten zusammen mit passend konstruierten Terminals erreichen lässt. Solche ,,passive" Karten weisen physikalische Echtheitsmerkmale wie z.B. Landis & Gyr-optische Codierungsstrukturen auf.

Einführung

Was bedeutet schon ein Name? ,,Was uns Rose heisst, wie es auch hiesse, würde lieblich duften." Vielleicht stimmt es, aber jeder Werbefachmann hätte Shakespeares Julia erklären können, dass es viel leichter sei, Rosen zu verkaufen als zum Beispiel ,,Dornblüten", wie ein schlecht gelaunter Botaniker sie hätte nennen können. Ein Name beeinflusst zwar keineswegs die Eigenschaft einer Sache, er kann aber bestimmt unsere Erwartungen an diese beeinflussen und unsere Reaktionen auf sie weitgehend steuern.

Man kann das Werbegenie nur bewundern, das den amerikanischen Spitznamen ,,smart card" (kluge Karte), erfunden hat, um damit die Mikroprozessorkarten zu beschreiben, die dank der Pionierarbeit des französischen Erfinders Roland Moreno (unter anderen) bereits in einigen Versuchssystemen angewendet werden [1,2]. Eine Plastikkarte, die nicht ,,smart" ist, kann nur dumm sein, und wer möchte gerne eine dumme Karte in seiner Tasche tragen? Aber der, einem späteren englischen Dichter entlehnte Gedanke, ,,Wo die Unwissenheit Glückseligkeit ist, da ist es Torheit, weise zu sein", sollte uns zur Vorsicht mahnen, bevor wir ohne weiteres die intelligente Karte als die beste Lösung bei allen Anwendungen für Plastikkarten akzeptieren.

Einen guten Ausgangspunkt für eine rationelle Betrachtung der Fähigkeiten und Grenzen der intelligenten Karten entnimmt man aus Julias darauffolgender Bitte an Romeo, ,,Leg' deinen Namen ab". Wenn man den Namen ,,smart card" weglässt, was findet man? – eine Plastikkarte in der ISO-Normengrösse ($85.7 \times 54 \times 0.76 \pm 10\%$ mm), die normalerweise einige gedruckte und aufgeprägte Daten aufweist und der ,,konventionellen" Kreditkarte sehr stark ähnelt. Jedoch bei näherer Betrachtung entdeckt man acht winzige elektrische Kontakte, die den Schlüssel zu dieser ,,ausserordentlichen" Karte darstellen.

Denn eingebettet in die Kunststoffschale versteckt sich ein Mikroprozessor, der diese acht Kontakte (möglicherweise gemeinsam mit zusätzlichen Speicherchips) benützt, um mit den Endgeräten, in die die Karte eingeschoben werden kann, zu kommunizieren. Sonst gibt es im Aufbau der intelligenten Karte nichts, was sie von ihren dummen Artgenossen unterscheidet. Je nach Anwendung könnte man fordern, dass die logischen Schaltungen das Schreiben in gewisse Speicherbereiche verhindern, und dass gewisse gespeicherte Codewörter geheimgehalten werden, oder ähnliches, aber dies sind Einzelheiten des Funktionskonzeptes, nicht Haupteigenschaften.

In der Folge wird eine Plastikkarte, die einen Mikroprozessor beinhaltet und an Terminals angeschlossen werden kann, als ,,intelligente Karte" oder ,,Mikroprozesorkarte" bezeichnet.

Bild 1 Optisch codierte Karten von Landis & Gyr

Bild 2 Chip-Karten

* Zentrale Forschung und Entwicklung,
LGZ Landis & Gyr Zug AG
CH-6301 Zug, Schweiz

** Institut für Signal- und Informationsverarbeitung,
Eidgenössische Technische Hochschule Zürich,
CH-8092 Zürich, Schweiz

Für welche Zwecke sind intelligente oder sonstige elektronische Karten besonders geeignet? Für welche Anwendungen bietet die Mikroprozessorkarte eine *zuverlässige, sichere* und *wirtschaftliche* Alternative gegenüber existierenden Kartentechnologien, wie der Landis & Gyr-optisch codierten Karte [3] oder der Magnetstreifenkarte? Das Ziel dieses Aufsatzes ist die Abklärung geeigneter und ungeeigneter Anwendungen für solche intelligente Karten.

Zu diesem Zweck ist der Artikel in zwei Hauptteile gegliedert. Im Teil I werden die wesentlichen Eigenschaften umrissen, die im allgemeinen bei Systemen mit Plastikkarten und insbesondere bei Zahlungssystemen anzutreffen sind. Vor allem werden die relevanten Sicherheitsanforderungen betrachtet.

Die Anwendung der im Teil I hergeleiteten zuverlässigen Konzepte auf Mikroprozessorkarten führt zwangsläufig zur Betrachtung kryptographischer Probleme, die zusammen mit elektronischen Karten und Kartensystemen im Teil II behandelt werden. In der Tat darf man behaupten, die Möglichkeit, Verschlüsselungs- und Entschlüsselungsoperationen innerhalb der Karte auszuführen, stellt die wichtigste neue Fähigkeit dar, die der Mikroprozessor seiner umschliessenden Plastikkarte verleiht.

Es wird gezeigt, dass intelligente Karten abgesichert werden können, sofern sie ihre „Verschlüsselungswerke" physisch schützen können. Jedoch erweist es sich, dass intelligente, mit Mikroprozessoren versehene Karten immer noch „taub" und „stumm" aus der Sicht ihrer Benützer bleiben. Deshalb erfüllen sie nicht alle erdenklichen Sicherheitsanforderungen, und zwar ausgerechnet für diejenige Anwendung, für die sie am meisten zu versprechen scheinen, nämlich für ungesicherte Terminals in einem Onlinesystem.

In der Tat kann man für solche Systeme wie auch für andere Anwendungen eine Alternative zur Mikroprozessorkarte finden, die bei gleicher Sicherheit bedeutend wirtschaftlicher ist. Man kann nämlich sichere, „passive" Karten, wie optisch codierte Karten, zusammen mit den entsprechend konstruierten Endgeräten verwenden. Deshalb ist es sehr fraglich, ob der höhere Preis der „aktiven" Karten für alle solche Anwendungen unbedingt gerechtfertigt ist.

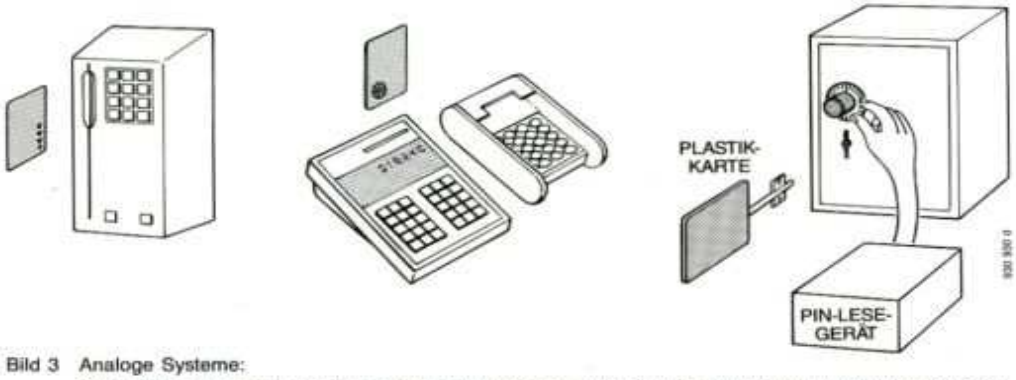

Bild 3 Analoge Systeme:
Zutrittskontrollsysteme und maschinell lesbare Kredit- oder Bankkartensysteme verwenden normalerweise individuell codierte Karten in Verbindung mit PIN-Codes (PIN = persönliche Identifikationsnummer), welche von den Benützern eingetippt werden müssen. Sie ähneln einem Schloss, das durch einen Schlüssel und das gleichzeitige Wählen einer dem Schlüssel entsprechenden Kombination geöffnet wird.

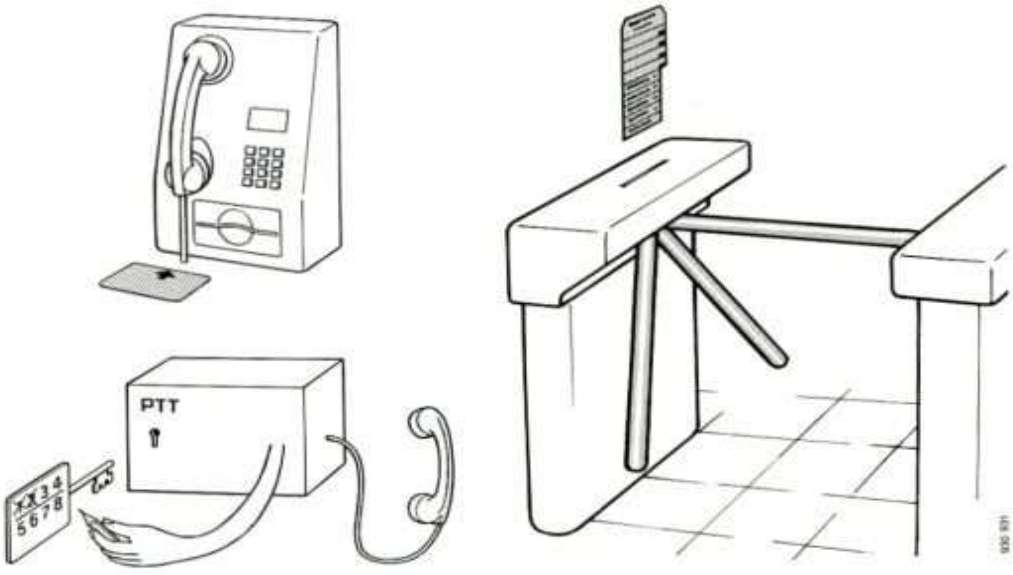

Bild 4 Analoge Systeme:
Vorbezahlte Telephonkarten und Mehrfahrtkarten werden beide während des Gebrauchs schrittweise entwertet. Bildlich dargestellt, öffnet die Telephonkarte dem Benützer das Telephon für Gesprächsverbindungen, die insgesamt dem auf der Karte vorhandenen Wert entsprechen. Die Entwertungen sollten irreversibel sein.

Teil I.
Kartensysteme für Zahlungs- bzw. Zutrittszwecke

1. Kartensysteme

Welche Vorteile bieten Kartensysteme? Genauer formuliert, weshalb werden maschinell lesbare Karten oft in Systemen eingesetzt, an die Sicherheitsanforderungen irgendwelcher Art gestellt werden? Die Antwort findet man am besten durch einen Vergleich zwischen modernen Kartensystemen und zwei ähnlichen Erfindungen aus der Antike: *das Schloss und der Schlüssel*, respektive *die Münze* im verallgemeinerten Sinne einer austauschbaren Marke. Maschinell lesbare Kartensysteme lassen sich allgemein in zwei Hauptkategorien aufteilen, je nachdem welche dieser Erfindungen sie nachahmen.

In vielen Systemen erfüllt die verwendete Karte eine ähnliche Funktion wie ein *Schlüssel* aus Metall, der mehrere Türen öffnen kann. Die Türen, ob im eigentlichen oder bildlichen Sinne, verschaffen den Zugang zu Gütern, Dienstleistungen oder Räumlichkeiten. Eine solche Karte ist normalerweise persönlich und, um Missbrauch durch Unberechtigte zu verhindern, wird dem Karteninhaber üblicherweise ein Passwort zugeteilt. Dieser sogenannte Inhaberkenncode oder PIN-Code (PIN = persönliche Identifikationsnummer), ist bei jeder Benutzung der Karte an der Tastatur eines Endgeräts einzutippen. Die dadurch erreichte zusätzliche Sicherheit, die charakteristisch für Kreditkarten-, direkte Debitkarten-, Bankautomat- und Zutrittskontrollsysteme wie das ID2000 [4] ist, entspricht dem Einbauen eines Kombinationsschlosses in eine Tür mit gewöhnlichem Schloss (siehe *Bild 3*). Die zwei Schlösser zusammen sorgen für höhere Sicherheit, als ein einzelnes.

Um Systeme, bei denen die Karte die Rolle einer Münze übernimmt, am besten zu verstehen, betrachtet man mit Vorteil einen besonderen Verwandten der Automatenmarke, nämlich den annulierbaren Jeton, dessen Wert ganz oder teilweise annuliert werden kann. Typische Beispiele sind Mehrfahrtkarten und Briefmarken. Bei solchen Kartensystemen werden unpersönliche, entwertbare Karten zum Gebrauch in Fernsprechern, Verkaufsautomaten, Parkhausautomaten und dergleichen verkauft. In einem gewissen Sinne funktionieren diese Karten wie temporäre Schlüssel, deren Gültigkeitsdauer allmählich während deren Gebrauch reduziert wird. Ein wohl bekanntes Beispiel ist das PHONOCARD System [5,6], das in mehreren europäischen Ländern in Gebrauch ist. Die Karte berechtigt ihre Benutzer dazu, für eine gewisse Anzahl Einheiten zu telefonieren. Die Werteinheiten werden während des Gesprächs annuliert (siehe *Bild 4*). Wem die für das Telefonieren erforderlichen Münzen einmal gefehlt haben, wird die

Vorteile solcher Karten zu schätzen wissen. Ausserdem entfällt wegen des Fehlens jeglichen Münzenbehälters am Apparat, das regelmässige Einsammeln der Einnahmen durch den Systembetreiber und die damit verbundenen Umtriebe. In der Folge werden nicht nur die Betriebskosten solcher Systeme gesenkt, sondern auch das Vandalismusrisiko wird beträchtlich reduziert.

In Wirklichkeit gilt leider unsere einfache Aufteilung nach Verwendungszweck nicht immer – einige der neueren Kartensysteme passen in beide Kategorien. Entwertbare Information auf einer Kreditkarte eignet sich dazu, allenfalls eine mit der Benutzung der Karte sinkende Kreditlimite aufzuzeichnen. Kreditkarten können auch mit einem vorausbezahlten Barwert für den Bezug gewisser automatisierter Dienstleistungen (wie z.B. lokale Telefongespräche) versehen sein, deren geringer Wert die mit der Bearbeitung von Kredittransaktionen verbundenen hohen Unkosten nicht rechtfertigt.

Der Leser wird sich an dieser Stelle wohl fragen, wieso man die herkömmlichen Kreditkarten mit Schlüsseln vergleicht. Selbstverständlich lässt sich die strenge Analogie nur auf Kreditkarten anwenden, die als Teil eines vollständig automatisierten Kartensystems betrieben werden. Die ursprünglichen Kreditkarten wurden als Identitätskarten konzipiert, die zusätzlich das einfache Drucken persönlicher Angaben auf Kreditbelege ermöglichen. Sie können etwa mit Pässen, Empfehlungsbriefen (eventuell mit besonderen Siegeln versehen), Bankkreditbriefen, um nur ein paar zu nennen, verglichen werden. Gewöhnliche Kreditkarten sind effektiv *Identitätsausweise*, welche die visuelle Prüfung bestehen müssen. Sie öffnen Türen, die nicht abgeschlossen sind, sondern von Portiers bewacht und bedient werden. Weitere bekannte Beispiele sind die Eurochequekarte und ähnliche Bankkarten. In diesem Artikel werden wir uns auf automatisierte Systeme beschränken; Echtheitsmerkmale, die für die Sichtkontrolle durch den Menschen bestimmt sind, werden in [7] beschrieben.

Welches sind die wesentlichen Eigenschaften maschinell lesbarer Kartensysteme? Zur Erläuterung dieser Frage dient die im *Bild 5* dargestellte Grundanordnung, bei der fünf Elemente erkennbar sind. Die *Karte* und das *Kartenlesegerät* sind für dieses Konzept unentbehrlich. Möglicherweise spielt auch der *Karteninhaber* eine aktive Rolle. Eventuell existiert ein getrennter *Zutritts- bzw. Dienstleistungsmodul*, der den Zugang zu den Räumlichkeiten oder Dienstleistungen überwacht; wie z.B. ein ferngesteuertes Türschloss. Schliesslich können die erwähnten Elemente an einem *zentralen überwachenden System* angeschlossen werden. Die zentrale Überwachung darf unterschiedlich komplex sein, von einer einzelnen Einheit bis zu einem ganzen Netzwerk.

Welche Aufgaben werden von den verschiedenen Komponenten übernommen? Zuerst muss das Kartenlesegerät (eventuell zusammen mit dem zentralen System) die *Echtheit* der verwendeten Karte feststellen. Zweitens müssen sachdienliche Angaben, wie z.B. die Identität des Karteninhabers oder ein Restwert, von der Karte *abgelesen* werden. Drittens ist es möglicherweise notwendig, mit Hilfe eines PIN-Codes, einer Unterschriftenprobe oder dergleichen die Identität des Kartenbenutzers zu *verifizieren*. Viertens müssen Restwertdaten bei Wert- oder gewissen Kreditkarten modifiziert werden. Schliesslich wird es möglicherweise erforderlich, verschiedene Daten zwischen einzelnen Systemkomponenten zu *übertragen*. Falls das Systemkonzept eine zentrale Überwachung einschliesst, müssen Informationen über die Karte, deren Inhaber sowie über allfällige Transaktionen der Zentrale übermittelt werden. Die Zentrale muss einen Befugnisentscheid zurücksenden. Ausserdem müssen dem allenfalls vorhandenen abgetrennten Dienstleistungsmodul die Betriebsanweisungen gegeben werden.

Die ersten zwei Schritte zusammen ermöglichen die *Gültigkeitsprüfung (Validierung)* der Karte. Sowohl ihre Echtheit wie auch ihr Befugnisbereich müssen kontrolliert werden. Die Befugniserteilung einer unpersönlichen Wertkarte hängt nur davon ab, ob der Restwert für die gewünschte Dienstleistung ausreicht. In einem Zutrittskontrollsystem umfasst der Befugnisbereich die Zugangsprivilegien eines Karteninhabers zu gewissen Räumlichkeiten während gewissen Zeiten.

Die Funktion einer zentralen Überwachung prägt die Eigenschaft des ganzens Systems. Ein System, das an einer Zentrale angeschlossen ist, wird als *Onlinesystem* bezeichnet, ohne Zentrale nennt man es *Offlinesystem*. Verglichen mit Offlineanlagen verfügen Onlinesysteme über leistungsfähige Hilfsmittel, welche die zuverlässige Kontrolle der Karten und Karteninhaber beträchtlich erleichtern können; z.B. durch Grosscomputer zugreifbare Datenbanken mit Kontoinformationen und Sperrlisten. In der Praxis werden die meisten Kartensysteme mit persönlichen Karten für den Online-Betrieb konzipiert. Zum Teil wird bei solchen Systemen sonst eine gemischte Betriebsart verwendet, falls die Verbindung mit der Zentrale nur für eine beschränkte Zeit zur Verfügung steht. Im Gegensatz dazu, werden Systeme mit unpersönlichen Karten im allgemeinen als Offlineanlagen konzipiert.

Die offensichtlichsten Schnittstellen in der im *Bild 5* dargestellten Grundanordnung beziehen alle das Kartenlesegerät mit ein. In einem Onlinesystem könnte man sich eine mögliche Kommunikationsschnittstelle zwischen der zentralen Überwachung und der Karte oder dem Karteninhaber vorstellen, die das Terminal effektiv umgeht. Eine weitere, wenn auch futuristische Möglichkeit, wäre eine direkte Kommunikationsschnittstelle zwischen der Karte und dem Karteninhaber, z.B. in der Gestalt einer Tastatur und einer Anzeige auf der Karte.

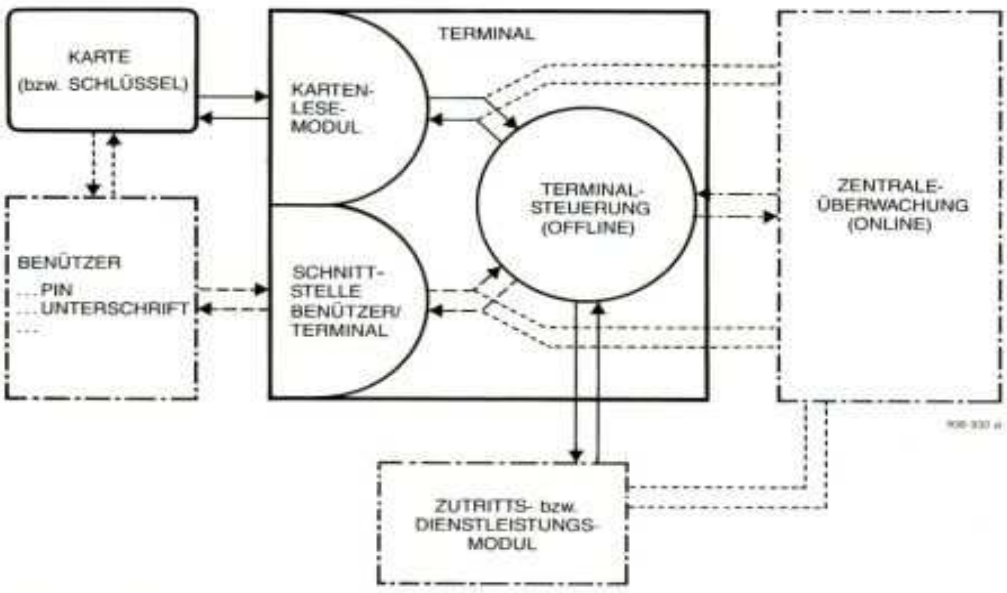

Bild 5 Die Grundkonfigurationen automatischer Zutritts- oder Dienstleistungssysteme:
Die unentbehrlichen Komponenten sind das *Terminal* und die *Karte*, deren Echtheit normalerweise durch das Kartenlesegerät geprüft wird. Zusätzlich könnte die Identität des *Benützers* verifiziert werden, falls z.B. der Benützer eine persönliche Identifikationsnummer am Terminal eingibt. In gewissen Fällen schliesst ein solches System einen getrennten *Zutritts- bzw. Dienstleistungsmodul* ein, der den Zutritt resp. die Dienstleistung steuert. Schliesslich könnten alle diese Konfigurationen noch mit einem *zentralen überwachenden System* verbunden sein, in dem Kontos oder schwarze Listen aufbewahrt sind.

2. Echtheit der Karte und Identität des Karteninhabers

Wie kann die Echtheit einer Karte im allgemeinsten Sinne geprüft werden? Gewöhnlich werden Karten mit Besonderheiten für

die visuelle Prüfung [7] zusammen mit Echtheitsmerkmalen für die maschinelle Prüfung versehen. Die letzteren können physikalisch messbare Eigenschaften oder in der Karte abgespeicherte codierte digitale Daten sein (der genaue Unterschied zwischen den beiden ist nicht immer klar definiert). Für die Echtheitsprüfung der Karte sind drei allgemeine Verfahren zu unterscheiden.

Erstens kann die Karte sich sozusagen beim Lesegerät vorstellen, in dem sie ihre Echtheitsmerkmale zur Prüfung unaufgefordert vorweist (man könnte dies das «Visitenkartenverfahren» nennen). Dies geschieht effektiv, wenn eine Magnetkarte durch ein Lesegerät («swipe reader») gezogen wird. Es wäre auch der Fall, wenn eine elektronische Karte beim Einschieben in das Lesegerät sich durch das sofortige Anbieten eines digitalen Passworts ausweisen würde.

Die zweite Methode könnte als ein Aufforderung/Antwort-Dialog zwischen der Karte und dem Terminal bezeichnet werden und entspricht dem Vorgehen militärischer Wachtposten. Das Lesegerät fordert die Karte auf, sich auszuweisen, und wertet die Antwort aus. Es wird angenommen, dass die Antwort von der Befragungsart abhängt, die ihrerseits variiert werden kann. Wie im *Bild 6* gezeigt, funktionieren Landis & Gyr-Kartensysteme gemäss diesem Prinzip. Die Karte wird optisch abgefragt und die Antwort, die sowohl von der optischen Information wie auch von der Beleuchtungsart abhängt, wird mit Hilfe eines optischen Detektorensystems ausgewertet (für Einzelheiten des letzten Schrittes, des Entscheides ob die Karte als echt betrachtet wird, siehe [8]). Im Teil II wird gezeigt, dass der Aufforderung/Antwort-Dialog die Grundlage für die Kommunikationsprotokolle darstellt, die für die Echtheitsprüfung intelligenter Karten geeignet sind.

Die dritte Variante lässt sich als ein «adaptiver Aufforderung/Antwort»-Dialog bezeichnen. Ähnlich einem Katechismus wird eine Folge von Aufforderungen gestellt und die entsprechenden Antworten bei jedem Schritt ausgewertet. Ausserdem kann die nächste Aufforderung von den vorhergegangenen Antworten abhängen.

Wie wird die Identität des Karteninhabers verifiziert? Es gibt zwei allgemeine Methoden, nämlich das Erkennen körperlicher Merkmale der Person und die Prüfung ihrer Kenntnisse. Die offensichtlich ideale Lösung wäre das einfache Erkennen des Karteninhabers. Es würde einem von einem Portier bewachten und zusätzlich noch abschliessbaren Eingang entsprechen. Leider gibt es keine Maschinen, die z.B. menschliche Gesichtszüge annähernd so gut erkennen wie Menschen es können (Analysen von Fingerabdrücken, Stimmen, Unterschriften und dergleichen sind Themen laufender Forschungsprojekte, die vielleicht eines Tages solche Maschinen ermöglichen werden). Deshalb werden die Kenntnisse des Karteninhabers geprüft, indem man von ihm verlangt, dass er einen PIN-Code oder ein sonstiges Passwort auswendig lernt.

Für die Verifizierung der Identität des Karteninhabers werden Verfahren angewendet, die den Methoden für die Echtheitsprüfung der Karte durchaus entsprechen. Die erste Variante ist die üblichste. Nachdem der Kartenbenutzer seine Karte in das Lesegerät eingeschoben hat, tippt er unaufgefordert seinen PIN-Code ein. Für die Identitätsprüfung ist eine Aufforderung/Antwort-Prozedur zwar nicht üblich, sie wird jedoch in gewissen Online-Kartensystemen verwendet, indem der Karteninhaber über familiäre Einzelheiten bisherige Käufe, usw. ausgefragt wird.

3. Wertdaten in Karten – entwertbare Karten

Weshalb gewinnt das PHONOCARD-System in mehreren europäischen Ländern verbreitete Anerkennung für zuverlässigen, sicheren und wirtschaftlichen Betrieb, während Berichte über Missbrauch die Versuche begleiten, welche die Magnetstreifentechnologie für ähnliche Anwendungen (einschliesslich Billettsysteme) einsetzen? Ist es möglich, für solche Anwendungen elektronische Karten

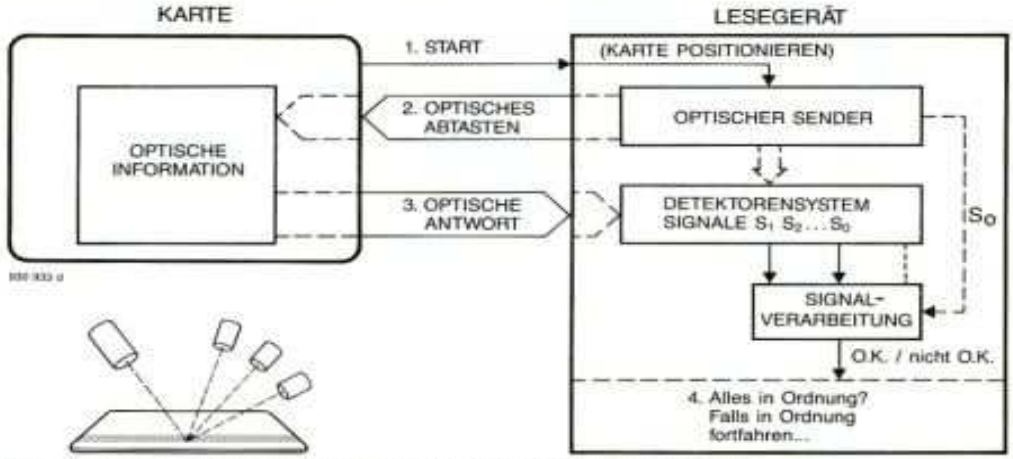

Bild 6 Die Art Echtheitsprüfung, die bei PHONOCARD-Systemen verwendet wird:
Das Lesegerät positioniert die Karte, tastet sie optisch ab und wertet die vom Detektorensystem empfangene Antwort aus. Die Antwort hängt sowohl von der optischen Codierung wie auch von der Beleuchtung ab.

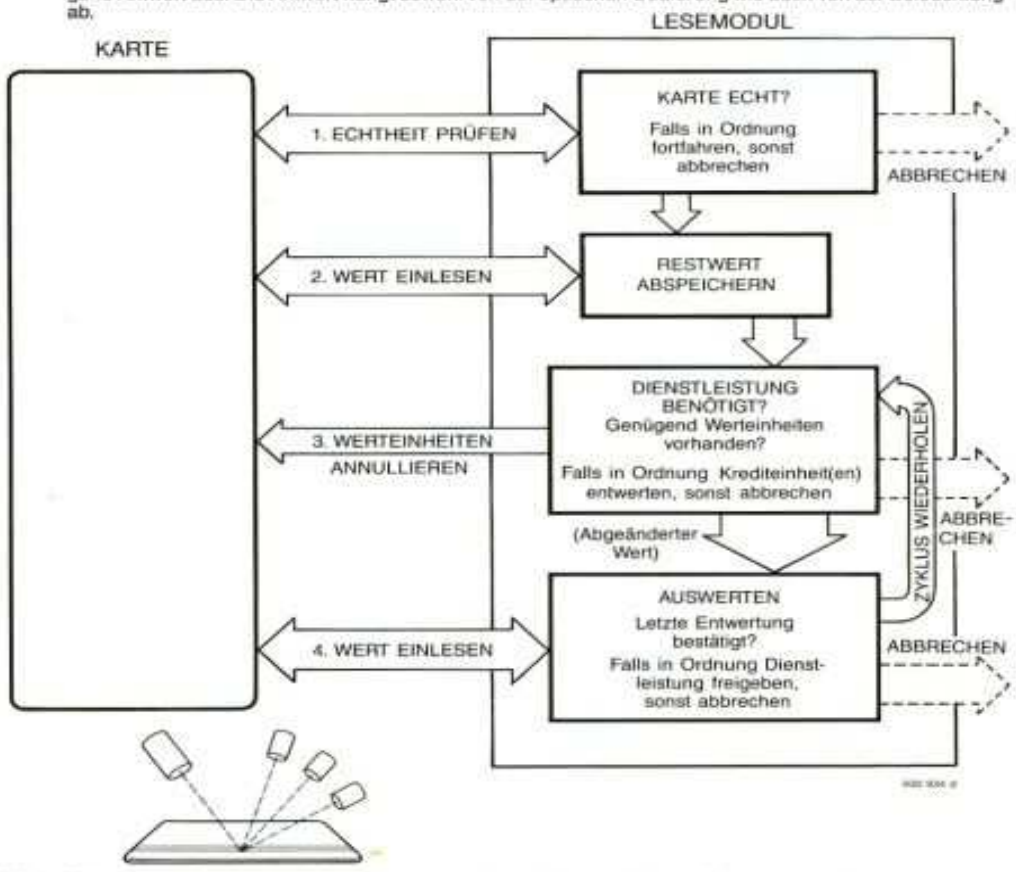

Bild 7 Beispiel der Gültigkeitsprüfung einer entwertbaren Karte und deren Entwertungszyklus.
Die einzelnen Schritte können Aufforderung/Antwort-Dialoge einschliessen. Die Gültigkeit wird in den Schritten 1 und 2 geprüft, der Entwertungszyklus besteht aus den Schritten 3 und 4. Im idealen Falle werden die Schritte 3 und 4 so oft wie praktikabel wiederholt und eine minimale Anzahl Einheiten bei jedem Zyklus entwertet. In einer anderen Anordnung könnte die Dienstleistung schon vor der Entwertung freigegeben werden.

zu verwenden? Tatsache ist, dass entwertbare Karten in Offlinebetrieben besondere Sicherheitsanforderungen stellen. Die PHONOCARD-Technologie wurde konzipiert, um diese Anforderungen zu erfüllen.

Was wird im allgemeinen von „Wertkarten" verlangt? Sie müssen mindestens elementare, maschinell lesbare Kontos irgendwelcher Art unterhalten; z.B. der übrigbleibende Barwert in einer vorbezahlten Karte oder die noch vorhandene Kreditbezugsgrenze in einer Kreditkarte. Bei normalem Gebrauch müssen die Kontodaten zuerst abgelesen und dann den Dienstleistungsbezügen entsprechend nachgetragen werden. Das wesentliche Problem betrifft die *Revision* solcher Kontos, nämlich die Gewährleistung, dass die Buchhaltung sich ausgleicht. Jede Kontomodifikation muss einer wirklichen Transaktion entsprechen. Auszuschliessen sind Modifikationen, die sich durch technische Defekte oder insbesondere durch betrügerische Manipulationen ergeben.

Zwei Buchführungsarten sind zu unterscheiden „reversibel" und „irreversibel". Reversible Buchhaltung schliesst sowohl Kredit- wie auch Debittransaktionen ein, irreversible Kontoführung sieht nur *eine* Transaktionsart vor. Letztere gilt für sogenannte *entwertbare* Karten, in denen ein sinkendes Guthaben nachgeführt wird; z.B. im PHONOCARD-System. Betrieblich gleichwertig sind Karten, die Bezüge aufzeichnen, wie z.B. die mit einfachen Speicherchips versehenen Telephonkarten eines Versuchsbetriebs. Die aufgebrauchten Karten werden weggeworfen. Hier muss betont werden, dass jedes System, das sogenannte „*wiederaufladbare*" Karten verwendet, die *reversible* Kontoführung mit einbezieht. Wiederaufladbare elektronische Karten sind geplant worden, aber sie wurden bisher nicht eingesetzt.

Welche Funktionen hat ein automatisiertes System durchzuführen? Bei normalem Gebrauch muss das Lesegerät die Kontoinformationen *ablesen* und *auswerten* (z.B. einen Restkredit notieren). Es muss die Daten den bezogenen Dienstleistungen entsprechend *modifizieren* und zudem *verifizieren*, dass die Modifikation durchgeführt wurde. Wie im *Bild 7* dargestellt, können diese Schritte zyklisch wiederholt werden. Die anfängliche Auswertung der Wertinformationen bildet einen Teil der gesamten *Gültigkeitsprüfung* der Karte. Jede Neuauswertung des Wertzustands bestätigt die vorherige Abänderung.

Steht die Authentizität der Karte fest, wäre es naheliegend, auch deren Informationen für echt zu halten. In der Tat sollten jedoch auch die Wertdaten auf ihre Echtheit hin geprüft werden, um jeglichen Betrug auszuschliessen. Effektiv geschieht dies im PHONOCARD-System, indem jedes Wertbit durch optisches Abtasten kontrolliert wird.

Wie werden die Daten modifiziert? Das hängt von der für deren Abspeicherung verwendeten physikalischen Technologie ab. Speichermedien können *reversibel* oder *irreversibel* abgeändert werden. Ersteres umfasst Systeme, in denen Informationen beliebig modifiziert werden können, entweder durch das Löschen und Neuschreiben oder durch das Setzen bzw. Annulieren einzelner Bits im Wertcode. Letzteres umfasst Systeme, in denen *entweder* das Setzen *oder* das Annulieren einzelner Bits möglich ist, jedoch nicht beides. Ein Vorteil reversibler Systeme ist die viel höhere verfügbare Informationsdichte. Ein 20-Bit-Wort gestattet die Codierung von ungefähr einer Million verschiedener Werte gegenüber den lediglich 20 Möglichkeiten in einem irreversiblen System.

Für die Abspeicherung von Informationen in entwertbaren Karten ist die einfachste und zuverlässigste Möglichkeit die Verwendung eines irreversibel veränderbaren Mediums. Im PHONOCARD-System z.B. bildet das selektive Löschen die einzig mögliche Modifikationsart. Elektronische Karten mit PROM-Speicher, auf die Daten unwiderruflich geschrieben werden, sind ebenfalls irreversibel. Die gegenwärtig erprobten, mit EPROM-Speichern versehenen Chipkarten sind in der Praxis auch irreversibel. Daten können auf unbeanspruchten Speicherplatz geschrieben aber nicht gelöscht werden. Wird statt dessen ein reversibel veränderbares Medium für entwertbare Karten eingesetzt, so wird es unvermeidbar mit der Achillesferse behaftet, dass Kartenbenutzer (oder im schlimmeren Fall ein Zweckverband von Kartenbenutzern) versuchen würden, verbrauchte Karten auf ihren vollen Wert aufzuwerten.

In Anwendungen mit reversibler Buchführung, z.B. bei aufladbaren Karten, können beide Speichermedien eingesetzt werden. Wird ein irreversibel veränderbares Medium verwendet, wie dies bei den gegenwärtigen Versuchssystemen der Fall ist, so muss ein besonderes Codierungssystem verwendet werden: die Kredit- und Debittransaktionen werden als unterschiedliche Eintragungen aufgeteilt und im typischen Fall in getrennte, reservierte Memorybereiche abgespeichert. Insbesondere müssen Eintragungen, die den Erwerb von Kredit aufzeichnen, vor allfälligem Missbrauch geschützt werden.

Die dritte Funktion ist die Kontrolle, dass Wertinformationen vorschriftsmässig abgeändert wurden. Um eine betrügerische Störung der Datenmodifikationen zu verhindern, *müssen* die neuen Informationen abgelesen und mit den vorgeschriebenen Daten verglichen werden. Vorzugsweise erfolgen das Modifizieren und entsprechende Verifizieren der Daten vor der Freigabe der Dienstleistungen. In Systemen mit Zeittaxierung, z.B. öffentliche Fernsprecher, sollten die Kosteninkremente womöglich in Echtzeit entwertet und verifiziert werden.

4. Sicherheit

Die entscheidende Frage, die bei den verschiedenen, für neue Anwendungen vorgeschlagenen Kartensystemen gestellt wird, lautet: „Wie sicher sind sie?". Um eine solche Frage zu beantworten, müssen die möglichen Sicherheitsgefahren analysiert, geeignete Gegenmassnahmen erwogen, und die Kartensysteme aufgrund der daraus resultierenden technischen Spezifikationen bewertet werden.

Um eine Gefahr für die Systemsicherheit abzuschätzen, sollten die folgenden Fragen abgeklärt werden: *welche* fragwürdige Handlung könnte vorgenommen werden (und durch wen)? *Wer* wird daraus Nutzen ziehen, und *wie und wo* wird das System gefährdet? Die Eigenschaft physischer Gefahren für die Sicherheit wie z.B. Vandalismus ist gut bekannt. Es soll deshalb hier nicht weiter darauf eingegangen werden. Statt dessen werden Fälle betrachtet, die auf irgendwelcher *Täuschung* basieren, nämlich *Betrug* in Kartensystemen für Zahlungszwecke und *unbefugter Zugang* in Zutrittskontrollsystemen.

Zunächst wird die ursprüngliche Frage etwas eingegrenzt. Welche Anforderungen müssen die verwendeten *Karten* erfüllen, um die Sicherheit eines Systems zu gewährleisten? Der Karteninhaber ist natürlich auch beteiligt. Deshalb werden für die in *Bild 5* dargestellte Systemanordnung Gefahren für die Sicherheit betrachtet, die die Karte und den Karteninhaber mit einbeziehen. Mögliche Gefahren, die das Kartenlesegerät, den Zutritts- bzw. Dienstleistungsmodul, oder die Onlinezentrale betreffen, werden bis zur Behandlung der intelligenten Karten im Teil II aufgeschoben.

Zwei Hauptkategorien von Missbrauch müssen betrachtet werden, nämlich die betrügerische Benutzung zweifelhafter Karten durch an und für sich legitime Kartenbenutzer, und der Missbrauch von Karten unter Vortäuschung einer falschen Identität des Benutzers, wie z.B. bei der Verwendung einer gestohlenen Karte. Im ersteren Fall bereichert sich der Karteninhabers auf Kosten des Systembetreibers, es sei denn er wird selber durch einen Dritten betrogen. Im letzteren Fall wird angenommen, dass ein unbefugter Benutzer entweder auf Kosten des legitimen Karteninhabers oder des Systembetreibers sich bereichert.

Wertkarten, vor allem unpersönliche vorbezahlte Karten, sind am gefährdetsten. Drei Hauptrisiken werden behandelt: die *Fälschung*, *Manipulation* und *Simulation* von Karten. Die Fälschung ist die unzulässige Herstellung von Kopien des Originals (in einem automatisierten System müssten nur diejenigen Kartenmerkmale genau kopiert werden, die vom System kontrolliert werden). Die Manipulation ist die betrüge-

rische Abänderung von vorhandenen Daten auf echte Karten, z.B. das unerlaubte „Wiederaufladen" einer verbrauchten Karte. Die Simulation ist die Konstruktion einer Karte, die die Funktionen des Originals nachahmt, sich aber technisch völlig davon unterscheiden kann.

Die obigen Sicherheitsgefahren gelten auch bei persönlichen Karten. Hinzu kommt nun jedoch noch ein viertes, schwerwiegenderes Problem, nämlich die betrügerische Benutzung einer echten Karte durch eine *unbefugte Person,* möglicherweise als Folge eines Kartendiebstahls. Wie bereits erwähnt, kann solcher Missbrauch durch die Verifizierung der Identität des Karteninhabers mit Hilfe eines Passworts, einer Unterschriftsprobe oder dergleichen verhindert werden. Wird es möglich, die Identität des Karteninhabers durch ein Onlinesystem zuverlässig zu kontrollieren, so kann folglich das Risiko, die Integrität der Karte zu kompromittieren, auf eine eventuelle Manipulation von Kartendaten wie Zutrittsprivilegien, Barwert-Kredite usw. eingeschränkt werden.

Um Fälschungen zu verhindern, bieten sich drei Alternativen an: erstens dafür zu sorgen, dass die *Herstellung* der Originale an sich *schwierig* ist, zweitens maschinell lesbare Merkmale zu verwenden, die für einen angehenden Fälscher *nicht erkennbar* sind, und drittens dafür zu sorgen, dass die *analytische Demontage* („backward engineering") der Karte, um ihre relevanten Sicherheitsmerkmale zu untersuchen, sich so *schwierig* wie möglich gestaltet. Die erste Forderung ist unentbehrlich. Um dafür zu sorgen, dass das Reproduzieren oder zumindest das wirtschaftliche Reproduzieren der Karte schwierig ist, sollten bei ihrer Herstellung sogenannte Schlüsseltechnologien verwendet werden. Geeignet sind Technologien also, die bei hohen Stückzahlen niedrige Produktionskosten verursachen, die jedoch unumgängliche hohe Anfangskosten bedingen. Beispiele sind sowohl die Landis & Gyr-optische Codierungstechnologie wie auch anwendungsspezifische integrierte Schaltungen. Die Fälschung elektronischer Karten wird zusätzlich erschwert, falls solche Karten mit besonderen Kommunikationsschnittstellen versehen werden, oder falls sie eine Elektronik besitzen, welche spezielle, bei üblichen Anwendungen nicht vorkommende Signalcharakteristiken aufweist. In der Praxis scheint jedoch die gegenwärtige Konzeptentwicklung für Chipkarte/Leser- Schnittstellen einer durchaus konventionellen Richtung zu folgen. Damit beabsichtigt man vermutlich die Senkung der Kosten für Kartenlesegeräte.

Durch die Verwendung „verborgener" Merkmale kann die Sicherheit zusätzlich erhöht werden. Dies sind Merkmale, die beim Inspizieren echter Originale nicht bemerkbar sind und deren Existenz soweit wie möglich geheimgehalten wird. Die Geheimhaltung verborgener Merkmale kann jedoch gefährdet werden, falls es angehenden Fälschern gelingt, ein Kartenlesegerät zu analysieren. Dies ist der Grund, warum Schlüsseltechnologien grundsätzlich verwendet werden sollten. Um die analytische Demontage zu verhindern, ist es zweckmässig, die Karten so zu konstruieren, dass die Demontage der Karte ohne gleichzeitige Zerstörung der Echtheitsmerkmale *unmöglich* ist. In Wirklichkeit wird dieses Ziel jedoch nicht immer erreicht.

Die möglichen Methoden, um unerlaubte Datenmanipulationen zu verhindern, hängen davon ab, wie die Daten modifiziert werden sollen. Permanente Karteninformationen, z.B. in einer persönlichen Karte, können auf einem irreversibel abänderbaren Speichermedium durch die Verwendung eines geeigneten Codierungsschemas geschützt werden. Codes mit einer festen Anzahl gesetzter Bit [8, 9, 10] ermöglichen das Schreiben der Information auf die Karte (durch selektives Löschen im Falle des ID2000 Systems), und sorgen gleichzeitig dafür, dass ein solcher Code nicht in einen anderen legitimen Code umgewandelt werden kann. Wird ein reversibel modifizierbares Medium verwendet, so kann durch die Verwendung kryptographischer Redundanz im Codierungsschema in Form von Meldungsauthentifizierungscodes (siehe nächster Abschnitt) die erfolgreiche Manipulation solcher Codes unwahrscheinlich gemacht werden. Der durch diese Methode erreichte Teilschutz muss in Bankautomatensystemen, welche Magnetkarten verwenden, mit einbezogen werden, weil die Karten sonst leicht zu manipulieren wären. Leider *verhindern diese Massnahme keineswegs das Kopieren echter Codes von anderen legitimen Karten.*

Wertdaten in einer entwertbaren Karte werden am besten durch die Verwendung eines irreversibel modifizierbaren Informationsträgers geschützt. Werden solche Daten trotzdem in einem reversibel abänderbaren Medium gespeichert, muss dafür gesorgt werden, dass der Kartenaufwertungsvorgang für den Karteninhaber technisch undurchführbar ist. Insbesondere muss das unerlaubte Kopieren eines höheren Wertes auf dieselbe Karte ausgeschlossen werden. Wie wird diese Forderung erfüllt? Weil das Kopieren aus dem *Lesen* und *Neuschreiben* der Daten besteht, sollte mindestens einer dieser beiden Vorgänge für den Laien undurchführbar sein. Die übliche Magnetstreifentechnologie ist für das Aufzeichnen annulierbarer Wertinformationen völlig ungeeignet, da magnetisch codierte Daten mit Hilfe mehr oder weniger üblicher Anlagen sowohl abgelesen wie auch neugeschrieben werden können.

Hier muss betont werden, dass die Anwendung kryptographischer Codierung für das Speichern von Wertinformationen keineswegs die obigen Forderungen erübrigt. In letzter Zeit wurden einige vergebliche Versuche unternommen, Wertdaten auf Magnetstreifen durch deren gemeinsame Verschlüsselung, in Verbindung mit dauerhaften, nicht abänderbaren und auf jeder Karte individuell codierten Daten, zu schützen. Für die Codierung der permanenten Daten werden unter anderem magnetische Wasserzeichen, fluoreszierenden Tinten, zufällige optische Eigenschaften des Papiers und dergleichen eingesetzt. Obwohl das Korrelieren von Wertdaten mit individuellen Karteninformationen die erfolgreiche Fälschung zu verhindern vermag, kann dieses keineswegs die *Manipulation* verhindern. Es genügt lediglich die gesamten Informationen des Magnetstreifens einer neuen Karte auf *dieselbe* zurückzukopieren, nachdem sie aufgebraucht worden ist – die Karte kann dann wiederverwendet werden.

Werden anstelle von entwertbaren Karten „wiederaufladbare" Karten verlangt, so ist die Situation ganz anders. Der Aufwertungsvorgang muss für den Karteninhaber technisch undurchführbar sein. Obwohl das „Zurücksetzen" einer Karte in ihren unverbrauchten Zustand durch die Verwendung eines irreversibel abänderbaren Mediums zwar verhindert wird, sind immer noch besondere Schutzmassnahmen erforderlich, um das Schreiben von Habeneinträgen in die für diesen Zweck reservierten Speicherbereiche zu verunmöglichen. Der einzige sinnvolle Zweck, der durch die Verwendung eines irreversibel abänderbaren Mediums erfüllt wird, besteht offenbar darin, die nachträgliche buchhalterische Revision solcher Karten zu ermöglichen. Die möglichen technischen Massnahmen für den Schutz solcher Krediteinträge werden in folgenden Abschnitten behandelt.

Das dritte Sicherheitsrisiko, das die betrügerische Benutzung maschinell lesbarer Karten durch einen sonst legitimen Karteninhaber beinhaltet, ist die Möglichkeit der *Simulation.* Bei Landis & Gyr-Systemen mit optisch codierten Karten tritt diese Problematik kaum auf, weil sich die relevanten optischen Eigenschaften nicht sinnvoll durch andere Technologien simulieren lassen – ein potentieller Fälscher müsste die Karten durch möglichst perfektes Reproduzieren der optischen Mikrostrukturen nachahmen. Bei auf *konventioneller Digitalelektronik* beruhenden Sicherheitsmerkmalen hingegen sind mannigfaltige Simulationsmöglichkeiten vorstellbar. Insbesondere könnte eine entwertbare Einwegkarte durch eine andere elektronische Karte simuliert werden, die für das bequeme Wiederaufladen durch ihren Besitzer konzipiert wurde.

Welche Schritte können unternommen werden, um solche Simulationen zu vereiteln? Eine Möglichkeit ist die Verwendung von *Schlüsseltechnologien* als Bestandteil des Konzepts. Beispiele sind besondere elektronische Betriebscharakteristiken oder die Verwendung einer optischen bzw. induktiven Karte/Leser-Schnittstelle. In

einer ,,anonymen" Umgebung wie z.B. in öffentlichen Fernsprechern, wo die Karten nicht einer visuellen Prüfung unterworfen werden, wird es ausserdem gegebenenfalls nötig, die Möglichkeit einer elektronischen Verbindung zwischen einer ,,Sklavenkarte" und einem intelligenten ,,Mastermodul" irgendwelcher Art auszuschliessen, indem allfällige Verbindungen dieser Art im Betrieb mechanisch *abgeschnitten* werden. Eine solche Massnahme wird nur dann notwendig, falls die Existenz einer unerlaubten Kommunikationsverbindung die Systemsicherheit gefährdet. Diese Massnahme ist für jedes Landis & Gyr-Kartensystem überflüssig; sie sind somit alle ,,benutzerfreundlich", indem der physische Zugriff zu der Karte dem Inhaber zu keiner Zeit vollständig verwehrt wird. Eine dritte Möglichkeit ist, die Merkmale, die simuliert werden können, *genügend komplex* zu gestalten, so dass die erfolgreiche Simulation sehr aufwendig gemacht wird. In den Prototypsystemen mit Mikroprozessorkarten wird diese Komplexität durch die Verwendung kryptographischer Protokolle erreicht.

Um die Dinge im richtigen Verhältnis zu sehen, gilt es zwischen den Forderungen der *Sicherheit* einerseits und jenen der *Zuverlässigkeit* und *Kundenfreundlichkeit* andererseits abzuwägen. Die hohe Sicherheit verlangt, dass die Wahrscheinlichkeit der Annahme ungültiger Karten so klein wie möglich gehalten wird, während die Betriebszuverlässigkeit verlangt, dass die Wahrscheinlichkeit der irrtümlichen Zurückweisung legitimer Karten möglichst gering gehalten wird. Deshalb muss die für Kartenechtheitsprüfung eingesetzte Technologie die Eigenschaft besitzen, dass beide Entscheidungsfehlerarten minimal sind. Abgesehen von dieser Wahl kann die Sicherheit nur auf Kosten der Zuverlässigkeit erhöht werden [8]. Um einen geeigneten Kompromiss zwischen Sicherheit und Zuverlässigkeit zu finden, muss das Risiko eines Marktverlustes, der sich als Folge von Kundenunzufriedenheit ergeben könnte, gegen die geschätzten Betrugsschäden abgewogen werden.

Welche Technologien auch immer verwendet werden, es bleibt noch die Frage der *administrativen Sicherheit*. Fallen Karten, Kartenlesegeräte oder deren Produktionsmittel in die falschen Hände, ist die Gesamtsicherheit des Systems ernsthaft gefährdet. Maschinell lesbare Karten müssen in zuverlässigen, sicheren Produktionsanlagen hergestellt werden. Diese Sorgfaltspflicht gilt auch für persönliche Karten, vor allem bevor sie mit individuellen Informationen codiert sind. Genauso wichtig ist es, für die richtige Installation und den einwandfreien Betrieb der Kartenlesegeräte zu sorgen (für weitere Details siehe [7].

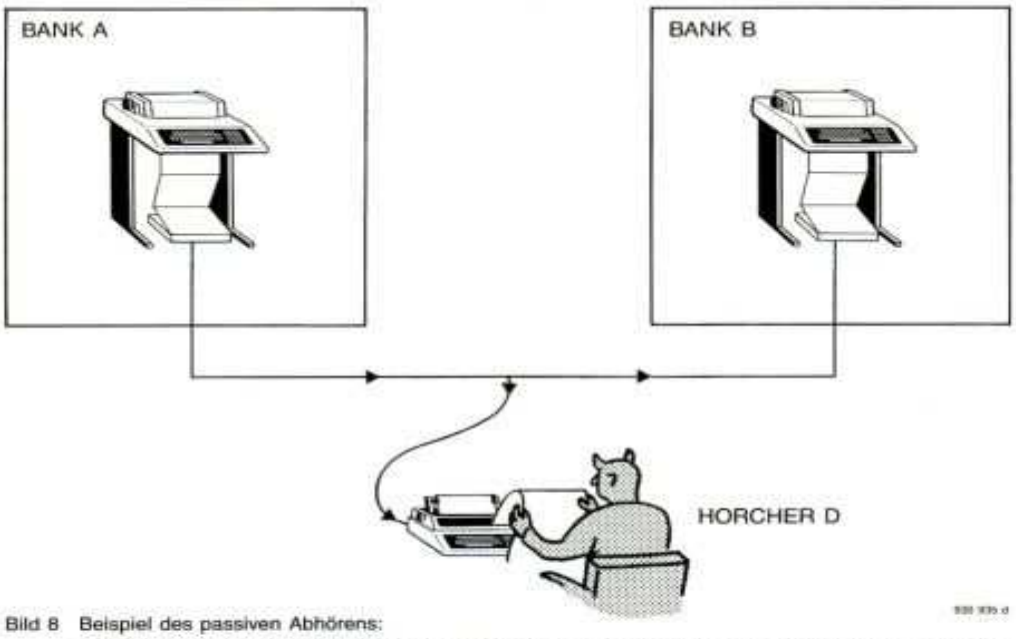

Bild 8 Beispiel des passiven Abhörens:
Telexnachrichten von der Bank A zur Bank B werden vom Horcher D abgehört. Zwar erreichen die Nachrichten B ohne Störung, aber deren *Geheimhaltung* wird in Frage gestellt.

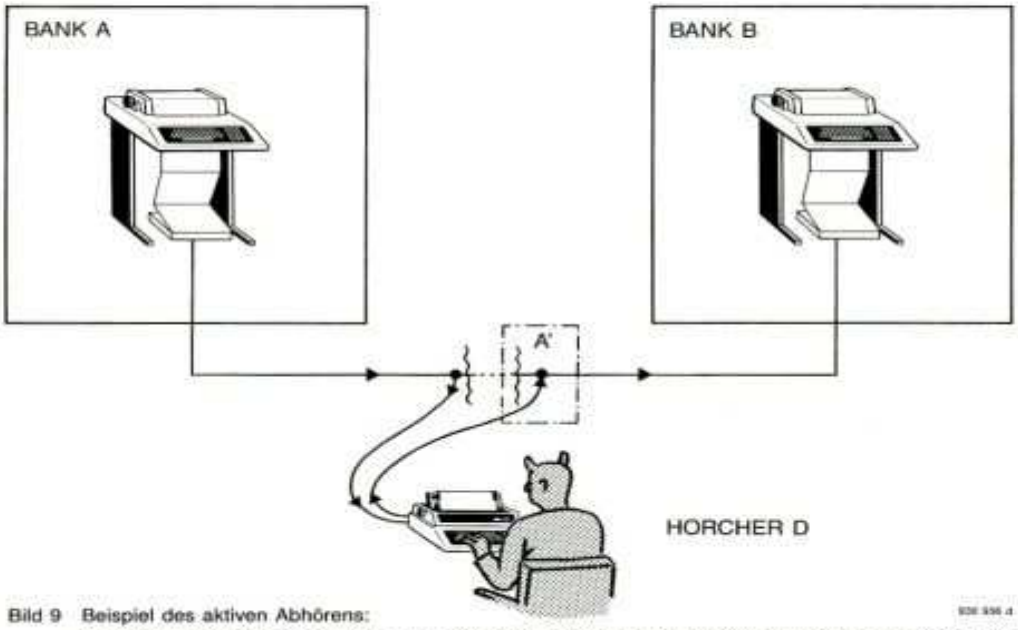

Bild 9 Beispiel des aktiven Abhörens:
Telexnachrichten von der Bank A zu der Bank B werden über einen Horcher D umgeleitet. Im einfachsten Falle bleibt der ursprüngliche Kanal bestehen, D schickt bloss zusätzliche Nachrichten an B. Andernfalls wird der ursprüngliche Kanal unterbrochen und D manipuliert den gesamten Nachrichtenverkehr von A nach B. Effektiv erhält B Nachrichten von einem fiktiven Sender A', der sich als A ausgibt. Nicht nur die Geheimhaltung, sondern auch die *Echtheit* der Nachrichten von A an B werden in Frage gestellt.

Teil II.
Der mögliche Beitrag der Kryptographie zur Sicherheit von Kartensystemen

1. Ein Exkurs: die Grundprinzipien der Kryptographie

Um genau zu verstehen, welche Vorteile kryptographische Methoden zur Sicherheit von Kartensystemen anbieten bzw. nicht anbieten, ist es notwendig, den allgemeinen Zweck und die Fähigkeiten der Kryptographie zu verstehen, und insbesondere, wie sie für die Echtheitsprüfung verwendet werden kann.

Der Leser, dem Zweck und Grundbegriffe der herkömmlichen sowie Public-Key-Kryptographie schon bekannt sind, kann diesen Abschnitt überspringen und direkt mit dem Abschnitt über die kryptographische Echtheitsprüfung beginnen. In diesem Abschnitt werden solche Begriffe wie Verschlüsselung, Entschlüsselung, Klartext, Geheimtext, Schlüssel, und im speziellen Public-Key-Kryptographie erläutert.

Die Kryptographie oder Geheimschrift kann als Spezialfall des allgemeineren Kommunikationsproblems der Informationscodierung betrachtet werden. Während die meisten Codierungsarten konzipiert sind, um die fehlerfreie Nachrichtenübertragung trotz der Anwesenheit des Rauschens zu gewährleisten, werden Meldungen kryptographisch codiert, um sie für mögliche Horcher *unverständlich* zu machen. Deshalb wird die Kryptographie auch treffenderweise als ,,Geheimcodierung" bezeichnet [11]. Dennoch erfüllt die

Kryptographie in Wirklichkeit zwei verschiedene Aufgaben, nämlich für die *Geheimhaltung* übermittelter Nachrichten zu sorgen und zudem deren *Echtheit (Authentizität)* nachzuweisen, was vor allem für diesen Artikel relevant ist.

Ein klassisches Szenario des Abhörens ist in *Bild 8* dargestellt. Eine Bank sendet einer anderen Bank via Telex Daten über vertrauliche Transaktionen. Gelingt es einem Horcher, die Telexleitung anzuzapfen und ihre Nachrichten auf seinem Terminal zu empfangen, erhält er Einblick in alle übermittelten vertraulichen Daten. Ein solcher Horcher wird als *passiv* bezeichnet, weil er die ungestörte Übermittlung von Daten zwischen den zwei Banken nicht direkt beeinträchtigt. Ein diabolischerer Feind ist der in *Bild 9* dargestellte *aktive* Horcher („spoofer"), der gegenüber seinem passiven Kollegen zusätzlich in der Lage ist, eigene Nachrichten an Bank B zu senden und möglicherweise auch die Übertragung legitimer Nachrichten zu unterbrechen. Er kann also Meldungen nach Bank B schicken, die von Bank A zu kommen scheinen. Er könnte z.B. Bank B anweisen, seinem dortigen Konto (oder dem eines Kollegen) eine passende Geldsumme gutzuschreiben. Auf subtilere Art könnte er eine Meldung von Bank A nach Bank B abfangen, lediglich den Geldbetrag abändern (selbstverständlich zu seinen Gunsten), und die Meldung dann weitersenden.

Um solche Irreführung zu vereiteln, können die Telexmeldungen von Bank A nach Bank B mit einem geheimen Codierungsverfahren *verschlüsselt* werden. Die ursprüngliche Meldung, der sogenannte *Klartext,* wird durch die Verschlüsselung in einen Chiffriercode, den sogenannten *Geheimtext,* umgewandelt. Der daraus resultierende Geheimtext wird von Bank B *entschlüsselt,* um die ursprüngliche Meldung wieder im Klartext zu erhalten. Der Geheimtext soll unverständlich sein und, solange der Horcher das Codierungsverfahren nicht kennt, wird er die Meldung nicht interpretieren können, und die Geheimhaltung ist gesichert. Versucht der Horcher ausserdem, eine eigene Meldung einzufügen, wird nach der Entschlüsselung derselben durch Bank B mit grösster Wahrscheinlichkeit nur sinnloser Text entstehen. Somit werden die verfälschten Daten erkannt. In diesem Falle ermöglicht der Gebrauch kryptographischer Methoden *sowohl* die Geheimhaltung wie *auch* die Gewährleistung der Authentizität.

Um unter vielen Benutzern, die die gleichen kryptographischen Codierungsprinzipien anwenden, gegenseitige Sicherheit zu gewährleisten, machen die meisten kryptographischen Transformationen Gebrauch von sogenannten *Schlüsseln,* welche die Benutzer geheimhalten. Mathematisch ausgedrückt ist der Geheimtext C eine Funktion sowohl des Schlüssels K wie auch des Klartexts M:

$$C = E_K(M) \quad (1)$$

Um den Klartext wiederherzustellen, muss die dechiffrierte Funktion D zusammen mit dem Umkehrschlüssel K*, der K entspricht, bekannt sein:

$$M = D_{K^*}(C) \quad (2)$$

Obwohl D und E einander offensichtlich komplementieren müssen (ebenso K* und K), gibt es *a priori* keinen Grund, dass D der Funktion E gleicht, oder schliesslich dass K* und K ähnlich sind. In der Praxis jedoch sind viele Chiffrierungsverfahren *symmetrisch* – d.h. die Verschlüsselungs- und Entschlüsselungsfunktionen sowie die Schlüssel K und K* sind praktisch gleich. Das historische Enigma-Verfahren, das von der deutschen Wehrmacht im Zweiten Weltkrieg verwendet wurde [12], und das moderne DES-Verfahren („Data Encryption Standard") [13], sowie die meisten Bitstromchiffriermethoden sind symmetrisch. Trotz der verschiedenen praktischen Vorteile, die symmetrische Verschlüsselungsverfahren bieten, wird in der Folge gezeigt, dass auch die Asymmetrie zweckmässig sein kann.

Eine typische kryptographische Anordnung ist in *Bild 10* dargestellt. Die Meldungen von Bank A werden mit Schlüssel K chiffriert und dann von der Bank B mit dem passenden Schlüssel K* dechiffriert, welcher über einen besonders abgesicherten Kanal nach B übertragen werden muss. Die *Geheimhaltung* der Nachrichten wird gewährleistet, solange der Horcher nicht Formel (2) anwenden kann, um sie zu *entschlüsseln*. Die *Echtheit* der Nachrichten wird gesichert, sofern (i) der Horcher nicht Formel (1) anwenden kann, um solche Meldungen zu *verschlüsseln,* und (ii) genügende Redundanz im Nachrichtenverkehr (im allgemeinen Doppelverkehr) vorhanden ist, damit B verifizieren kann, dass keine falschen Meldungen eingeschleust wurden.

So theoretisch gut fundiert diese Grundprinzipien auch sind, gibt es leider zahlreiche Beispiele von genialen Chiffrierverfahren, die genauso genial geknackt wurden [14]. Die Kunst und Wissenschaft der *Kryptologie* umfasst zwei Hauptgebiete, die *Kryptographie* und die *Kryptanalyse* – die Anwendung respektive die Analyse von Chiffriermethoden. Eine unerlässliche Zielsetzung bei der Konzipierung eines Chiffrierverfahrens ist dafür zu sorgen, dass es dem Horcher nicht gelingt, durch raffinierte Raterei die Verschlüsselungs- oder Entschlüsselungsvorgänge herauszufinden. Kryptanalytische Angriffe werden je nach Voraussetzung in drei Stufen unterteilt. Auf der ersten Stufe ist der Kryptanalytiker lediglich in der Lage, den Nachrichtenverkehr abzuhören und Geheimtextmeldungen zu beobachten – der *Geheimtext*-Angriff. Auf der zweiten Stufe kennt der Kryptanalytiker zumindest einen Teil des entsprechenden Klartexts – der *bekannte Klartext*-Angriff. Auf der dritten Stufe kann der Kryptanalytiker zumindest einen Teil der im Klartext gesendeten Nachrichten wählen – der *gewählte Klartext*-Angriff. In dieser Situation kann der Kryptanalytiker eine Tabelle der Klartext/Geheimtext-Paare, ein sogenanntes elektronisches Codebuch (ECB), zusammenstellen. Falls er zudem die Verschlüsselungsfunktion kennt, kann er versuchen, den verwendeten Schlüssel herauszufinden.

Obwohl es durchaus üblich ist, vor allem bei militärischen Anwendungen *alle* Einzelheiten über die Chiffriermethoden zu verschweigen, ist es bei manchen Anwendungen im öffentlichen Sektor unpraktisch, die Verschlüsselungs- und Entschlüsselungsalgorithmen geheimzuhal-

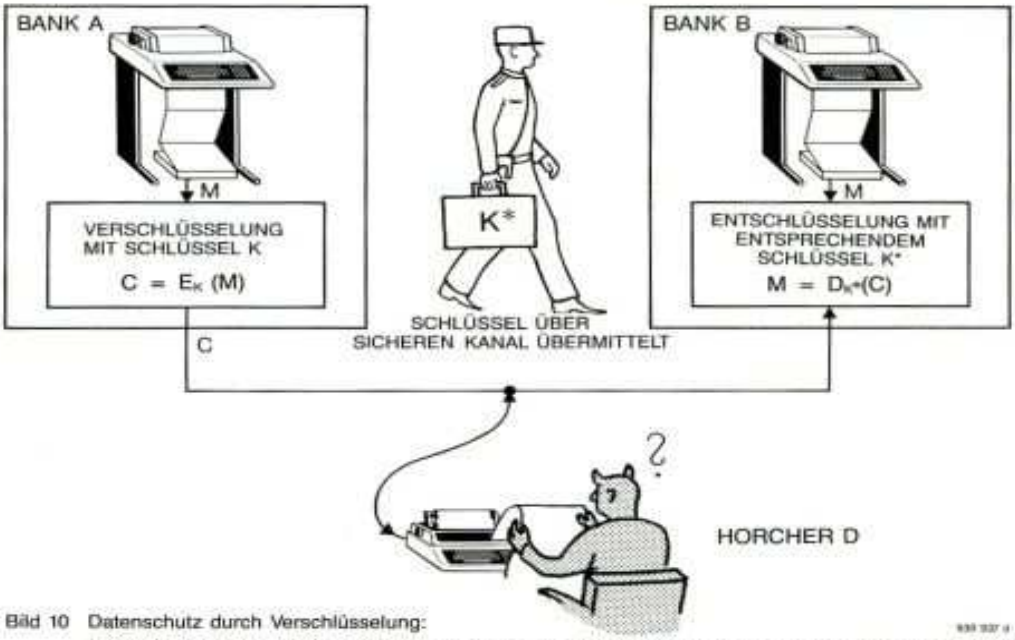

Bild 10 Datenschutz durch Verschlüsselung:
Die Meldung M von A wird mit dem Schlüssel K verschlüsselt. Der daraus resultierende Geheimtext ist dem Horcher D unverständlich, kann jedoch von B unter Anwendung des entsprechenden Schlüssels K* entschlüsselt werden, um die ursprüngliche Nachricht heraus zu bekommen. Die *Geheimhaltung* wird gewährleistet, falls K* dem Horcher D unbekannt bleibt. Die *Echtheit (Authentizität)* der Meldungen von A oder die Identität von A kann mit Hilfe geeigneter Protokolle verifiziert werden, solange K dem Horcher unbekannt ist.

ten. Deshalb sollte ein gutes kryptographisches Verfahren auch gegen einen Angriff mit gewählten Klartext, bei dem der Gegner über alle Details des Chiffrierprozesses, ausser den geheimen Schlüsseln, orientiert ist, gesichert sein. Im idealen Fall sollte dem Gegner keine effizientere Möglichkeit zur Verfügung stehen, als ein *ausführliches Durchsuchen* durch alle möglichen Schlüssel, bis der richtige gefunden ist. Das DES-Verfahren [13] wurde nach dieser Spezifikation konzipiert und soll einen Gegner dazu zwingen, 2^{56} verschiedene Schlüssel durchzusuchen. Dass diese Zielsetzung wirklich erfüllt wird, ist theoretisch nicht nachgewiesen; trotzdem wird der DES-Algorithmus allgemein als starkes Chiffrierverfahren erachtet. Eine offensichtliche, zusätzliche Voraussetzung für die Sicherheit ist die *Integrität der Hardware*, in der der Schlüssel gespeichert wird. Hat ein Gegner Zugang zur Chiffriereinheit und die Möglichkeit den Schlüssel direkt auszulesen, wird das zuverlässige Konzept des Verfahrens völlig nutzlos.

Um die durch eventuelle Preisgabe von Schlüsseln resultierende Verwundbarkeit zu minimalisieren, ist es eine gute Praxis, die Chiffrieralgorithmen geheimzuhalten. Diese Massnahme verhindert jedoch die kritische Bewertung kryptographischer Verfahren durch ihre Anwender und könnte mögliche Schwächen verbergen. Paradoxerweise könnte die Geheimhaltung der in Mikroprozessor-Kartensystemen verwendeten Verschlüsselungsalgorithmen in der kommerziellen Anwendung für Skepsis über das angebotene Sicherheitsniveau sorgen, obwohl dies in der militärischen Praxis akzeptiert wird.

Auch wenn die Geheimhaltung der Chiffrier- und Dechiffrierfunktionen garantiert wird, muss von der Voraussetzung ausgegangen werden, dass ein Kryptanalytiker versuchen könnte, durch die Zusammenstellung von Klartext/Geheimtext-Paaren ein elektronisches Codebuch zusammenstellen. Betrachtet man die Verschlüsselungsfunktion als die Substitution eines Blocks Geheimtext für einen Block Klartext, so sollte die minimale Blocklänge gross genug sein, damit eine solche Tabellarisierung unpraktikabel wird. Die im DES-Verfahren verwendete Blockgrösse von 64 Bit würde genügen.

Der Betrieb kryptographischer Systeme bedingt die sichere Administration der verwendeten Schlüssel, die sogenannte *Schlüsselverwaltung*. Erstens müssen die Schlüssel an kryptographische Module verteilt werden, ohne ihre Geheimhaltung zu gefährden. Zweitens und nicht weniger wichtig, müssen Schlüssel von Zeit zu Zeit *ausgewechselt* werden. Damit wird das Risiko verringert, dass sie aufgedeckt oder unabsichtlich preisgegeben werden. Wie oft sie erneuert werden sollten, hängt sowohl von dem für ihre Entdeckung benötigten kryptanalytischen Aufwand, wie auch von der Tragweite der Folgen, die aus dem Kompromittieren eines bestimmten Schlüssels resultieren würden, ab.

Grosses Interesse hat die jüngste Entwicklung und Einführung der sogenannten *Public-Key-Kryptographie*, die „öffentliche" Schlüssel verwendet, erweckt [15,16]. Die Public-Key-Algorithmen entsprechen der obigen Beschreibung, sie sind jedoch extrem *asymmetrisch* in dem Sinne, dass die Kenntnis von K nicht reicht um K* (oder möglicherweise umgekehrt) zu bestimmen, ausser durch ausführliche Durchsuchungsmethoden. Eine Funktion E mit dieser Eigenschaft wird oft als eine Einwegfalltürfunktion („one way trap door function") bezeichnet, weil die explizite Umkehrfunktion von E_K, nämlich D_{K^*}, nicht von E abgeleitet werden kann, sondern nur dann bestimmt werden kann, falls die Falltür K* *von vorneherein* bekannt ist [15,16]. So paradox dies erscheinen mag, ist die Idee nicht sehr unterschiedlich von der Forderung, einen gewöhnlichen Schlüssel gegen Angriffe mit gewähltem Klartext zu schützen. Genau wie K aus bekannten (M,C) Paaren ausschliesslich durch gründliche Versuche mit Formel (2) herausfindbar sein sollte, wird an einen Public-Key-Algorithmus eine ähnliche Forderung gestellt. Der bestechende Unterschied besteht darin, dass K zwar bekannt ist, aber trotzdem keine Abkürzung der Bestimmung seines asymmetrischen Gegenstücks K* ermöglicht.

Das erste Public-Key-Verfahren wurde von Rivest, Shamir und Adleman 1978 vorgeschlagen [17]. Dieser sogenannte RSA-Algorithmus gilt heute noch als der beste. Es sei $n = pq$ das Produkt zweier sehr grosser unterschiedlicher Primzahlen, und es sei $\phi(n) = (p-1)(q-1)$ die Euler'sche Totientfunktion von n [18]. Man wähle die zwei Zahlen e und d, so dass sie zu $\phi(n)$ prim sind und folgender Gleichung genügen:

$$e\,d = 1 \bmod \phi(n) \qquad (3)$$

(Der Ausdruck $a = b \bmod k$ heisst, dass die Differenz von a und b ein Mehrfaches von k ist). Es sei m die Zahl, die eine Meldung M im Klartext darstellt. Dann wird c,

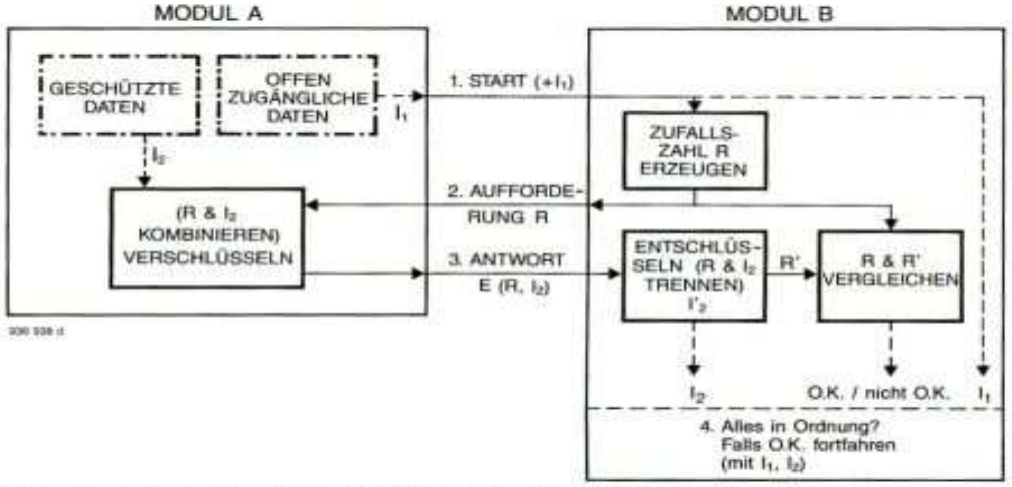

Bild 11 Ein typisches Authentizitätsprüfverfahren mit expliziter Auswertung der Antwort:
Das *Modul B* prüft die Authentizität vom *Modul A* durch das Senden einer Zufallsbitfolge R, die von A verschlüsselt wird und als Chiffrat zurück an B übermittelt wird. Die Meldung wird von B *entschlüsselt* und das Ergebnis mit der ursprünglichen Bitfolge R verglichen. Daten könnten auch von A an B übermittelt werden, entweder als Klartext während des 1. Schrittes oder als Geheimtext während des 3. Schrittes. A könnte wohl eine Mikroprozessorkarte und B ein Kartenlesemodul darstellen.

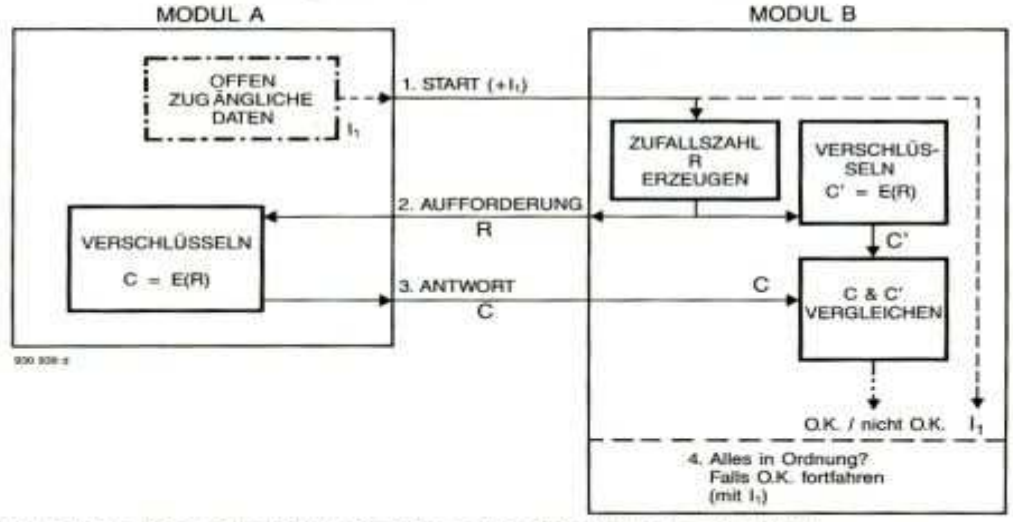

Bild 12 Ein typisches Authentizitätsprüfverfahren mit impliziter Auswertung der Antwort:
Das *Modul B* prüft die Authentizität vom *Modul A* durch das Senden einer Zufallsbitfolge R, die von A verschlüsselt wird und als Chiffre zurück an B übermittelt wird. Gleichzeitig *verschlüsselt* B die Bitfolge R und vergleicht das Ergebnis mit der von A empfangenen Chiffre. Dieses Verfahren gestattet die Anwendung von irreversiblen Chiffrierungsalgorithmen.

die den Geheimtext C darstellende Zahl, von m durch die Formel errechnet:

$$c = m^e \bmod n. \quad (4)$$

Um die Meldung zu dechiffrieren wird

$$m' = c^d \bmod n, \quad (5)$$

berechnet, welches zu

$$m' = m^{1+a\phi(n)} \bmod n \quad (6)$$

äquivalent ist. Sofern m und n zueinander prim sind, müssen nach dem Fermat'schen Satz [18] m und m' modulo n identisch sein. Da p und q gemäss Voraussetzung unterschiedlich sind, gilt in der Tat $m' = m$ für *alle* m. Also kann die ursprüngliche Klartextmeldung immer erfolgreich wiederhergestellt werden.

Falls nun n und e veröffentlicht werden, während d (und p & q) geheimgehalten werden, scheint es effektiv unmöglich zu sein, d aus e abzuleiten. Die Primzahlen p und q müssen lediglich gross genug gewählt werden (z.B. jede mit ungefähr 100 Dezimalstellen), um zu gewährleisten, dass die Teilerzerlegung von n nicht durchführbar ist, auch nicht mit einem Aufwand von Jahren von CPU-Zeit auf den modernsten Computern. Wird n nicht zerlegt, so kann $\phi(n)$ nicht berechnet werden und folglich kann e nicht aus d (und umgekehrt) bestimmt werden.

Ein solches Schema bietet die *Geheimhaltung* der Nachrichten an, weil nur der legitime Empfänger in der Lage ist, eine Meldung aus dem Geheimtext zu entschlüsseln, obwohl der Chiffrierungsschlüssel (n,d) öffentlich bekannt ist. Umgekehrt können d (und p & q) geheimgehalten werden, während das Paar (n,e) veröffentlicht wird. Dies würde die *Echtheitsprüfung* ermöglichen. Nur der legitime Sender ist in der Lage, eine im voraus vereinbarte Meldung zu verschlüsseln und damit effektiv eine digitale Unterschrift zu erzeugen, obwohl jeder Empfänger sie verifizieren kann. Eine der bemerkenswerten Eigenschaften der Public-Key-Kryptographie ist diese klare Unterscheidung zwischen den zwei Hauptzwecken der Kryptographie, nämlich das Sorgen für Geheimhaltung und Authentizität [11].

Die Anwendung der Public-Key-Kryptographie kann die *gegenseitige* Anfälligkeit konventioneller System umgehen. Durch die Preisgabe eines Schlüssels folgt nicht unbedingt die Bekanntgabe der Schlüssel allfälliger Kommunikationspartner. In Public-Key-Systemen muss ein fauler Apfel in der Umgebung kryptographischer Module nicht hundert andere anstecken. Ferner braucht jeder Benutzer eines Public-Key-Systems nur einen einzigen geheimen Schlüssel aufzubewahren, verglichen mit mehreren Schlüsseln in symmetrischen Kryptosystemen.

2. Authentifizierung

Eine der wichtigsten Folgerungen, die aus den vorangehenden Abschnitten gezogen werden kann, ist, dass die Kartensystemsicherheit eng mit den Echtheitskontrollen verbunden ist. Kryptographische Methoden können solche Kontrollen anbieten. Das Verifizieren der Authentizität beinhaltet nicht nur die kryptographischen Algorithmen, sondern auch irgendein *Erkennungskriterium* irgendwelcher Art. Ein von Modul A nach Modul B gesendeter Authentifizierungscode muss mit anderen Informationen, die B besitzt, übereinstimmen. Entweder müssen A und B im voraus über geteilte geheime Informationen verfügen, die A nach B im Geheimtext übermitteln kann, oder die Referenzdaten müssen irgendwie zwischen den beiden Modulen übertragen werden.

Wird die Echtheit aufgrund gemeinsamer, im voraus vereinbarter Informationen geprüft, so wird ein dynamischer Wechsel notwendig. Ein einfaches Passwort trägt das Risiko, dass es durch einen Horcher aufgezeichnet und wiederverwendet werden kann. Eine Methode, die für genügende Variabilität sorgt, ist die Verschlüsselung von Zeit und Datum. Bei einer anderen Methode werden die Schlüssel in einer aufeinander abgestimmten Sequenz erneuert. Dieses Konzept eignet sich für feste Verbindungen in einem Netzwerk, in welchem eine Koordination zwischen den Knotenpunkten durchführbar ist [19]. Im Gegensatz dazu ist diese Methode völlig unpraktikabel für Kartensysteme, bei denen die Karten nicht mit Uhren versehen werden können und die Reihenfolge möglicher Kommunikationen zwischen Karten und Terminals nicht voraussehbar ist.

Deshalb muss die zweite Möglichkeit analysiert werden, nämlich die Übermittlung der für die Echtheitskontrolle notwendigen Informationen. Eine stillschweigende Voraussetzung dafür ist eine gewisse *Redundanz* im Nachrichtenverkehr zwischen A & B. Eine Möglichkeit wäre, dass A eine Meldung verschlüsselt und ihr einen entsprechenden redundanten Kenncode beifügt. Der daraus resultierende Geheimtext wird nach B übermittelt. Ein Beispiel dieser Art kryptographischer Redundanzkontrolle ist das Beifügen sogenannter Meldungsauthentifizierungscodes (MAC = „message authentification code") zum anfänglich erzeugten Geheimtext. Wird es jedoch A gestattet, sämtliche für die Kontrolle benötigte Informationen zur Verfügung zu stellen, so können die Nachrichten aufgenommen und später abgespielt werden, ohne dass B dies bemerkt.

Ein sinnvolleres Konzept ist der Gebrauch eines Aufforderung/Antwort-Protokolls. Angenommen, Modul B will die Authentität vom Modul A kontrollieren. Zuerst fordert B durch Senden eines zufälligen Klartexts A zur Verschlüsselung auf, und kontrolliert dann, ob A den entsprechenden Geheimtext richtig zurücksendet. Wie in *Bild 11* dargestellt ist, können die Verschlüsselung und Entschlüsselung getrennt verwendet werden, falls A zusätzliche Informationen im zurückgesendeten Geheimtext einschliesst. Sonst kann eine implizite Kontrolle mit Einwegchiffrierung verwendet werden; das entsprechende Schema ist in *Bild 12* dargestellt. Es muss auch für das gelegentliche Auswechseln von Schlüsseln gesorgt werden, jedoch ist es unpraktikabel, alle Schlüssel eines Kartensystems gleichzeitig zu erneuern. Deshalb sollten Authentizitätskontrollen so durch-

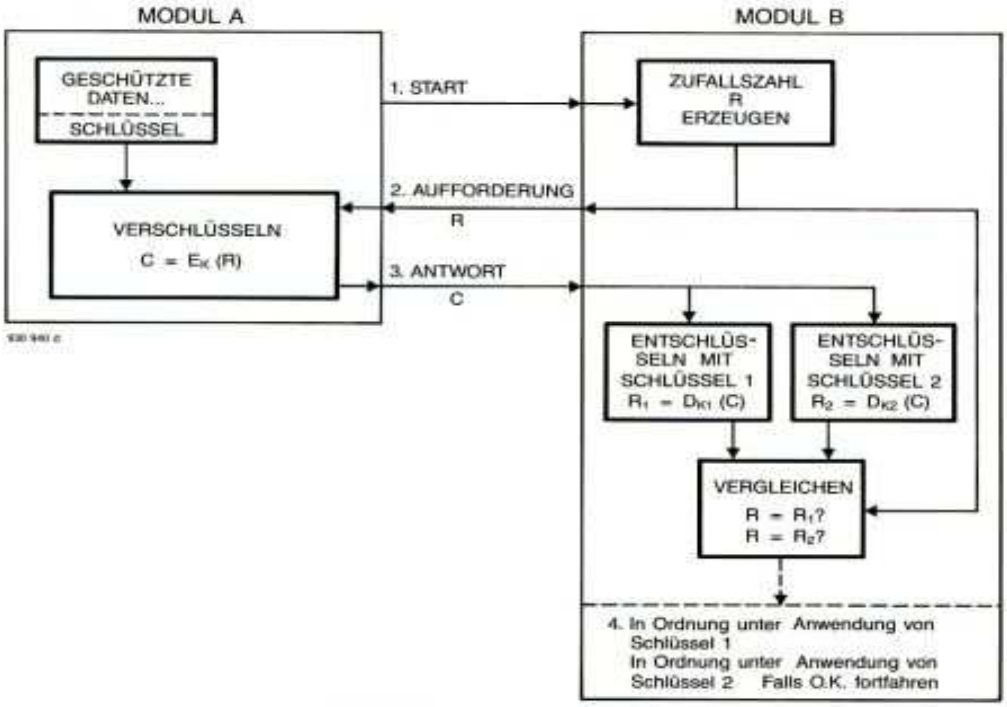

Bild 13 Ein typisches Authentizitätsprüfverfahren, das die Verwendung von mehr als einem Schlüssel erlaubt:
Das *Modul B* prüft die Authentizität vom *Modul A* unter Berücksichtigung der Möglichkeit, dass A die Schlüssel K1 oder K2 usw. verwenden kann. Die daraus resultierende implizite Identifikation von A's Schlüssel könnte auch noch mit anderen von A gelieferten Daten verglichen werden. Die implizite Authentizitätsprüfung wäre genau so gut möglich. Dieses Verfahren gestattet das allmähliche Ersetzen eines Schlüssels durch einen anderen.

geführt werden, dass während den Übergangsperioden mehr als ein Schlüssel als gültig erkannt werden (*Bild 13*).

Die Sicherheit eines solchen Protokolls hängt von zwei Dingen ab, nämlich der Sicherheit des Chiffrierverfahrens und der *Zufälligkeit* des mit der *Aufforderung* zum Chiffrieren gesendeten Klartexts. In der Folge werden solche Aufforderungen zum Chiffrieren einfachheitshalber lediglich als Aufforderungen bezeichnet. Verfügt ein Kryptanalytiker über gewählte Klartext/Geheimtext-Paare, und ist er zudem in der Lage, die Aufforderungen im voraus zu bestimmen oder zu beeinflussen, so wird er sie auch simulieren können. Theoretisch ideale Aufforderungen wären wirklich zufällig; sie könnten z.B durch die Analog/Digital-Umwandlung elektronischen Rauschens erzeugt werden. Jedoch ist die Welt nicht ideal, und die Forderung von Zuverlässigkeit und Wirtschaftlichkeit führt zur Verwendung von *Pseudozufallzahlen*. Zu diesem Zweck können z.B. die nichtlinearen Rückkopplungsschieberegister, die für die Erzeugung von Pseudozufallsbitfolgen für Bitstromchiffriermethoden verwendet werden, eingesetzt werden.

Welche Methoden auch immer für die Erzeugung von Zufallszahlen verwendet werden, ist es unerlässlich, dass deren Generation *zuverlässig* und gegen *Einflüsse von aussen* gefeit ist. Es wäre kaum befriedigend, wenn der Zufallsgenerator versagen und wiederholt die gleiche Zahl liefern würde. Deshalb brauchen solche Geräte eine *Fehlerschutzvorrichtung*, so dass bei einer allfälligen internen Panne keine Zahlen ausgegeben werden. Zudem muss das Zurücksetzen des Pseudozufallsgenerators in einen anfänglichen Zustand verunmöglicht werden, ansonsten eine vorher beobachtete Folge von Zufallszahlen wiederholt werden könnte.

Ist es möglich, die Public-Key-Kryptographie in dieser Situation zu verwenden? In der Tat liegt eine vielversprechende Anwendung der Public-Key-Kryptographie in der Erzeugung sogenannter digitaler Unterschriften. Die bereits beschriebenen Verfahren können mit einer zusätzlichen Verfeinerung dazu gebracht werden, dass das Modul dessen Authentizität geprüft wird, einen geheimen Schlüssel verwendet, während das Modul, das die Kontrolle durchführt, den entsprechenden öffentlichen Schlüssel benutzt. Deshalb kann Modul A eine zu authentifizierende Meldung mit einem geheimen Schlüssel verschlüsseln, und *jedes* Modul des Systems kann sie mit dem entsprechenden öffentlichen Schlüssel entschlüsseln. Erweist sich die dechiffrierte Nachricht als richtig, so konnte sie *nur* durch A erzeugt worden sein.

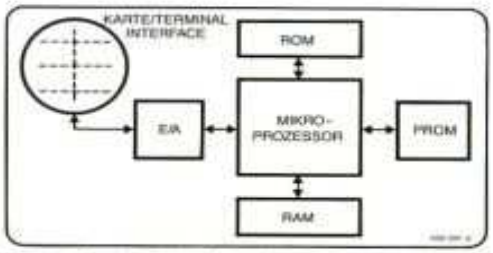

Bild 14 Symbolische Anordnung innerhalb einer Mikroprozessorkarte:
Der Zugriff zu den verschiedenen Speicherkomponenten wird durch den Mikroprozessor verwaltet. Im idealen Falle sollten sich der Mikroprozessor und die gezeigten Speicher auf demselben VLSI Chip befinden.

Auf den ersten Blick scheinen Public-Key-Authentifizierungsmethoden zusätzliche Sicherheit in Situationen bieten zu können, in denen mit der Gefährdung eines der Schlüssel zu rechnen ist. Modul B kann die Authentizität von Modul A kontrollieren, und, auch wenn der Schlüssels von Modul B aufgedeckt wird, bleibt die Geheimhaltung des entsprechenden von Modul A verwendeten Schlüssels bestehen. Jedoch ist die Sache nicht so einfach wie sie erscheint. Die Sicherheit hängt von der Art des Erkennungskriteriums ab. Sofern Modul B den Inhalt der von A gesendeten Authentifizierungsmeldung nicht beeinflussen kann, ist es möglich, die digitale Unterschrift von A zu fälschen. Dies bedingt, dass die Meldungen im voraus vereinbarte, dynamisch variierende Daten wie Sequenzzahlen, Tageszeit usw. mit einbeziehen.

Werden Public-Key-Verfahren in Zusammenhang mit Aufforderung/Antwort-Protokollen gebraucht, hängt die angebotene Sicherheit von der Art der von B gesendeten Aufforderungen ab. Sind diese im voraus berechenbar, und kann ein aktiver Horcher Modul A ausfragen, um die geeigneten Antworten im Geheimtext zu erhalten, so könnte er B täuschen. Notwendig ist die Verwendung entweder eines betriebsicheren Echtzufallszahlengenerators oder eines zuverlässigen, *geheimen* Pseudozufallszahlengenerators. Wird die Erzeugung von Pseudozufallszahlen verwendet, so müssen folglich *beide* an einer Authentizitätskontrolle beteiligten Module geheime Daten schützen. Diese Anforderung lässt sich keineswegs durch den Gebrauch der Public-Key-Kryptographie umgehen.

In erster Linie bietet die Public-Key-Kryptographie für die Sicherheit eine Begrenzung des Ausmasses potentieller Anfälligkeit. In einem konventionellen Kryptosystem würde die Preisgabe des Schlüssels von Modul B in der Folge auch den Schlüssel von A enthüllen, was die Simulation von A nach *jeder* Authentifizierungsaufforderung ermöglichen würde. Werden Public-Key-Methoden verwendet, so würde der Schlüssel von A trotzdem noch geheim bleiben, und lediglich diejenigen Module könnten getäuscht werden, die Aufforderungen nach dem gleichen Verfahren wie B erzeugen.

3. Mehr oder weniger intelligente elektronische Karten

Es ist an der Zeit, auf die spezifischen Eigenschaften von Mikroprozessoren einzugehen. Wie funktionieren intelligente und weniger intelligente Karten eigentlich? Elektronische Karten halten sich an die ISO-Standarddimensionen für Kreditkarten, sind zudem (gegenwärtig links oben) mit acht metallischen Kontakten versehen, die mit den in der Karte eingebetteten elektronischen Schaltungen verbunden sind. Die Elektronik kann einen Speicher, mit oder ohne zusätzlichen Mikroprozessor, oder einen einzelnen VLSI-Chip („very large scale integrated circuit"), der Mikroprozessor und Speicher enthält, umfassen. Alle diese Karten, die auch als *Speicherkarten* („cartes à mémoire") bezeichnet werden, teilen die Eigenschaft, dass sie mit keiner internen elektrischen Speisung versehen sind und dass die Speicher notwendigerweise nichtflüchtig sind. Für das Lesen aus dem Speicher und das Schreiben in den Speicher ist eine externe Stromversorgung erforderlich. Die acht Kontakte sorgen demgemäss sowohl für die Herstellung der Kommunikationsverbindung mit dem Terminal wie auch für die für den Betrieb der Karte benötigte Speisung.

Es können vier Arten von standardisierten nichtflüchtigen Speichern eingesetzt werden: ROM, PROM, EPROM und EEPROM. Wie der Name sagt, ist das eigentliche ROM („read only memory") nur lesbar. Es wird mit fest einprogrammierten Daten in grossen Stückzahlen hergestellt und kann nicht nachträglich abgeändert werden.Das PROM („programmable read only memory") ist *irreversibel* abänderbar. Es lässt sich nämlich programmieren, indem selektierte, interne leitende Verbindungen von passend hohen Strömen durchgebrannt werden. In das EPROM („erasable programmable ROM") kann durch Anlegen genügend hoher Spannung (21–25 V verglichen mit 5 V für Kommunikationszwecke) selektiv geschrieben werden. Obwohl dieser Speicher auch noch als „löschbar" bezeichnet wird, ist dieser Vorgang irreversibel in dem Sinne, dass *selektives* Löschen ausgeschlossen ist, obwohl das Löschen des gesamten Bereichs durch ultraviolettes (UV) Licht mög-

Geheimer Bereich (nur lesbar) nur dem Mikroprozessor zugänglich	PIN Kryptographischer Schlüssel Sicherheitsprogramme
Geschützter Bereich (Les- und schreibbar) Durch Mikroprozessor verwaltet	Statusangaben Karteninhaberangaben Transaktionen
Frei zugreifbarer Bereich (nur lesbar)	Herstellerangaben
(Les- und schreibbar)	Notizen vom Karteninhaber

Bild 15 Symbolische Organisation des Speichers der Mikroprozessorkarte:
Die PIN-Codes, Authentifizierungskennzahlen und ähnliches dürfen nicht von ausserhalb der Karte zugreifbar sein. Deshalb befinden sie sich in einem geheimen Bereich. Kontodaten müssen sorgfältig in einem geschützten Bereich unterhalten werden, dessen Inhalt jedoch von ausserhalb der Karte lesbar ist. Schliesslich können Informationen, die keinen Sicherheitsforderungen unterworfen sind in einem frei zugreifbaren Bereich gespeichert werden.

lich ist. Schliesslich bietet das EEPROM („electrically eraseable PROM") die Möglichkeit, den Speicher rein elektrisch zu löschen.

Die Prototypen elektronischer Kartensysteme, die gegenwärtig in Betrieb sind, benutzen alle entweder PROM- oder EPROM-Komponenten. In der Praxis müssen die mit EPROM versehenen Karten gegen unabsichtliches bzw. mutwilliges Löschen geschützt werden, was zur Folge hat, dass sie überhaupt nicht gelöscht werden können. Solche Karten speichern ihre Daten also in einem *irreversibel abänderbaren* Medium (in der Zukunft werden zudem möglicherweise hybride EEPROM-Chips entwickelt, die nicht-löschbare Bereiche einschliessen). Abgesehen von der Tatsache, dass die eine elektronische Karte durch eine andere simuliert werden kann, könnten PROM- bzw. EPROM-Speicherkarten als zufriedenstellende entwertbare Karten eingesetzt werden. Bei Anwendungen, die sowohl Kredit- wie auch Debiteinträge auf der gleichen Karte vorsehen, gibt es jedenfalls weitere Sicherheitsprobleme, die gelöst werden müssen. In der Folge wird gezeigt, dass der Mikroprozessor der intelligenten Karte eine mögliche Lösung bietet, sofern er richtig eingesetzt wird. Die Verwendung von Karten mit EEPROM- bzw. EAROM-Chips* verspricht, die Regeneration verbrauchter Karten zu ermöglichen. In der Folge wird jedoch gezeigt, dass ein Mikroprozessor auch hier benötigt wird, um genügende Sicherheit zu gewährleisten.

Es sollte trotzdem betont werden, dass jedes System für das „Auffrischen" aufgebrauchter Karten an sicheren, authorisierten Anlagen zwangsläufig beträchtliche administrative Unkosten mit sich bringt. Es ist wichtig, diese Unkosten gegen jene der Versorgung und Verteilung neuer Karten abzuwägen. Erstere sind derart hoch, dass sich das Wiederaufladen von Karten niedrigen Wertes, z.B. Telephonkarten, als sehr unwirtschaftlich erweist. Das Wiederaufladen rechtfertigt sich nur für diejenigen Karten, die zwischen Regenerationen im Zusammenhang mit grösseren Geldumsätzen gebraucht werden. Angesichts der hohen administrativen Unkosten und potentiellen Sicherheitsrisiken, könnte es sich herausstellen, dass das Ersetzen solcher Karten günstiger ist als das Wiederaufladen.

Die im allgemeineren Sinne genannte „intelligente" Karte umfasst, zuzüglich ihrer Speicherkomponenten, entweder eine fest verdrahtete Logikschaltung oder einen Mikroprozessor. Eine fest verdrahtete Logikschaltung sorgt normalerweise für rechnerische Effizienz, während ein Mikroprozessor flexibler ist und es erlaubt die gleiche Mikroprozessorkarte für unterschiedliche Anwendungen anzupassen. Ein vereinfachtes Schema der Mikroprozessorkarte ist in *Bild 14* dargestellt. Ein wesentliches Merkmal ist die vollständige Steuerung des Zugriffs zu den Speichern durch den Mikroprozessor. Dies ermöglicht die administrative Aufteilung des Speichers nach dem in *Bild 15* dargestellten Schema. Ein *geheimer Bereich* wird benötigt, weil von solchen Karten gefordert wird, dass sie in der Lage sind, Chiffrierungsvorgänge vorzunehmen. Sie müssen deshalb geheime Schlüssel (oft als Authentifizierungscodes bezeichnet) im Memory abspeichern können. Der Mikroprozessor muss unbedingt dafür sorgen, dass externe Lese- bzw. Schreibbefehle nicht diesen Speicherbereich adressieren können. Auch der für die *Buchhaltung* benötigte Speicherbereich muss geschützt werden, obwohl die darin gespeicherten Daten vom Terminal abgelesen werden können. Sind Kredit- anstatt Debiteinträge in der Karte zu notieren, ist offensichtlich besonderer Schutz beim Schreiben erforderlich. Schliesslich kann ein *offener,* verhältnismässig ungeschützter Bereich für Anwendungen eingesetzt werden, bei denen in der Praxis keine Gefährdung zu erwarten ist.

Im Hinblick auf das hohe Datenspeichervermögen intelligenter Karten ist eine Anwendungsmöglichkeit dieser Art naheliegend. Sie können nämlich als *elektronisches Notizbuch,* in dem Informationen für den persönlichen Gebrauch des Karteninhabers abgespeichert werden, dienen. Weitere denkbare Anwendungen sind unter anderen ein elektronisches Scheckheft oder eine Telephonkreditkarte, die ein Verzeichnis häufig angerufener Telephonnummern enthält.

Die Achillesferse aller elektronischer Karten ist die Möglichkeit, einen Kartentyp mit einem anderen zu simulieren. Das Kartenlesegerät kann nicht wissen, was unter den acht Kontakten verborgen ist, ausser durch die Art und Weise, wie die Elektronik der Karte auf elektronische Anregungen antwortet. Falls die von der Karte zurückgesendeten Signale keine unnachahmbare physikalische Echtheitsmerkmale (im Sinne der analogen Elektronik) besitzen, besteht die offensichtliche Alternative, dass die Antwort der Karte eine nicht leicht nachahmbare *digitale* Komplexität aufweist. An dieser Stelle kommen die in den vorangehenden Abschnitten beschriebenen Chiffrierverfahren zur Anwendung.

Das erste in Angriff zu nehmende Problem ist, wie ein Kartenlesegerät die Echtheit der Karte prüfen kann. Hier wird auf die in Abschnitt 4 vom Teil I beschriebenen Authentifizierungsmethoden hingewiesen. Als erste Möglichkeit könnte die Karte ein digitales Passwort anbieten, sobald die Speisung eingeschaltet wird. Es wäre jedoch nicht ausserordentlich schwierig, eine Karte dazu zu veranlassen, ihr Passwort an ein Aufnahmegerät abzugeben. Es wäre dann möglich, falsche Karten so zu programmieren, dass sie das richtige Passwort vorweisen. Um Schutz gegen geniale, technisch begabte Bastler („hackers") zu bieten, sollte offensichtlich ein Aufforderung/Antwort-Protokoll verwendet werden, indem eine unvorhersehbare Zufallszahl vom Terminal gesendet und eine chiffrierte Antwort von der Karte zurückgesendet wird. Die im letzten Abschnitt beschriebenen und in den *Bildern 11* bis *13* dargestellten Protokolle finden hier direkte Anwendung, wobei Modul A die Karte und Modul B das Terminal darstellt. Das Terminal gibt eine unvoraussehbare Aufforderung ab und die Karte muss dazu mit einer richtig verschlüsselten Rückmeldung antworten.

Wie sicher ist diese Art von Echtheitskontrolle? Um diese Frage zu beantworten, muss erkannt werden, dass sich Mikroprozessoren von anderen Arten kryptographischer Module dadurch unterscheiden, dass sie dem Risiko irgendeines physischen Eingriffs extrem stark ausgesetzt sind. Chiffriermodule in Fernschreibern, Computern und dergleichen werden normalerweise regelmässig kontrolliert, und eine physische Störung würde fast sicher von der verantwortlichen Stelle bemerkt. Im Gegensatz dazu sind kommerziell verwendete Karten derart zahlreich, dass mit Verlust oder Diebstahl von mindestens einem kleinen Anteil der Karten im Umlauf zu rechnen ist, und dass einige der vermissten Karten einer technischen Analyse unterzogen werden. Ausserdem muss mit versuchtem elektronischem Abhören an

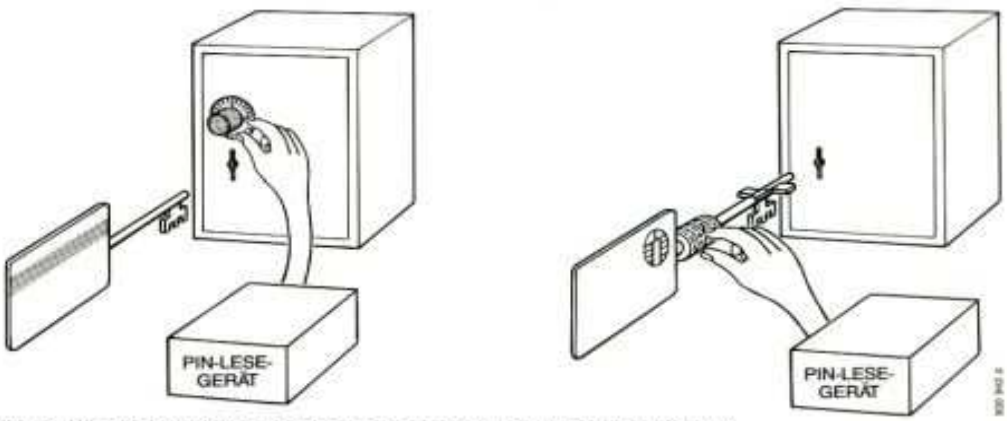

Bild 16 Wie die Mikroprozessorkarte die Identität des Karteninhabers verifiziert:
Der PIN-Code wird direkt in der Karte anstatt im Terminal kontrolliert. In Analogie zum Schlüssel von Bild 3 müsste das Kombinationsschloss nun durch einen besonderen Schlüssel, der selbst mit einer Kombinationsmechanik versehen ist, ersetzt werden. Die Kombination muss korrekt gewählt werden, damit der Schlüssel das Schloss öffnen kann.

* EAROM:
„electrically alterable ROM" – elektrisch abänderbarer ROM

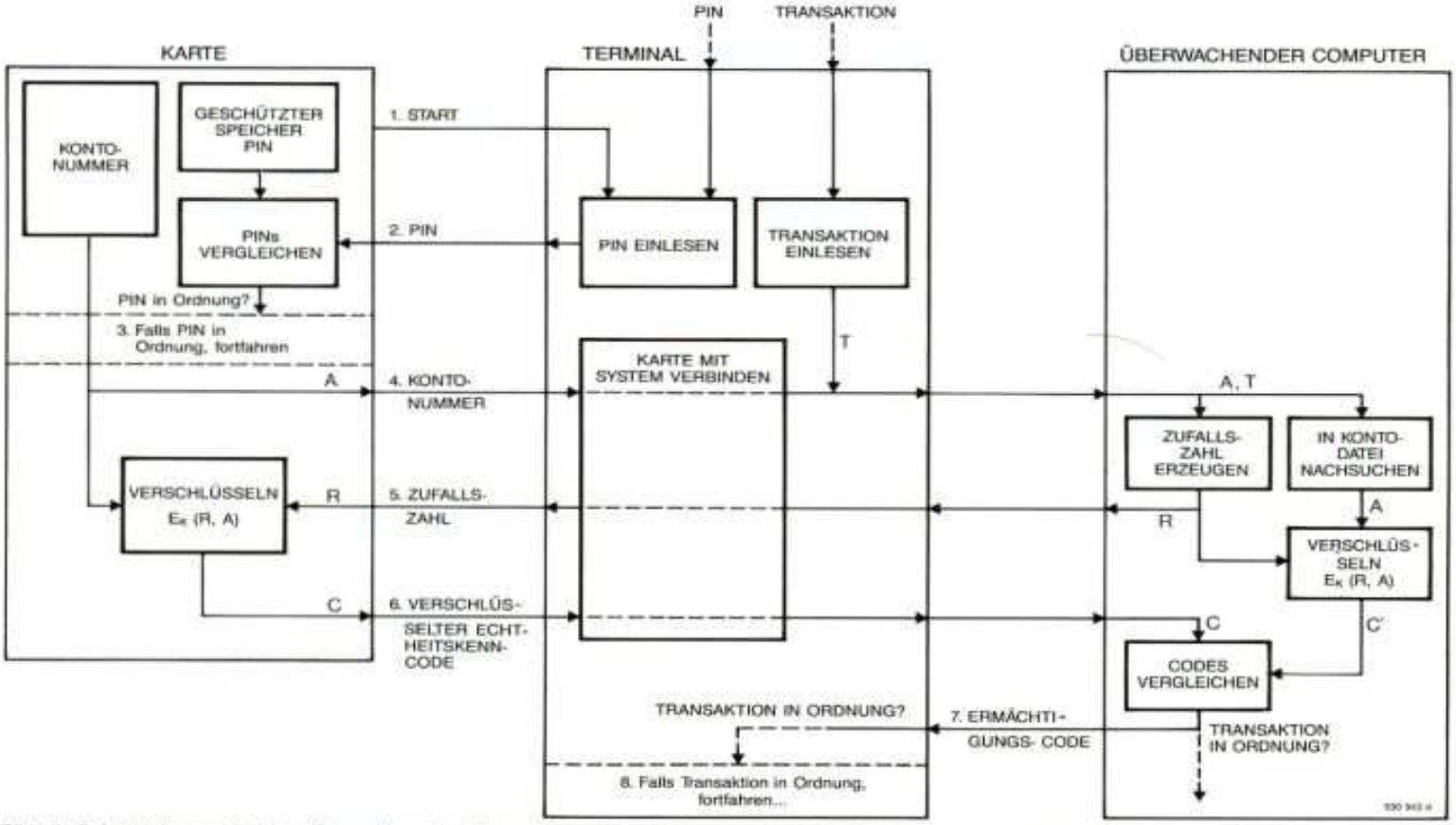

Bild 17 Beispiel des persönlichen Gebrauchs einer Mikroprozessorkarte an einem „online"-Terminal:
In den Schritten 1 bis 3 wird der am Terminal eingegebene PIN-Code innerhalb der Karte kontrolliert. Falls er richtig ist, gibt die Karte eine Kontonummer ab, welche an das System im Schritt 4 weitergeleitet wird. Im Schritt 5 sucht das System in der Kontodatei nach demjenigen geheimen Karteninhaberkenncode (Schlüssel), der auch im Geheimbereich der Karte abgespeichert ist, und sendet eine Zufallszahl als Aufforderung. Sobald das System die chiffrierte Antwort erhält, prüft es in den Schritten 6 und 7, ob sie mit der gesendeten Zufallszahl und dem geheimen Kenncode richtig verschlüsselt wurde, bevor es im Schritt 8 das Terminal ermächtigt, die Transaktion durchzuführen.

der Karte/Lesegerät-Schnittstelle gerechnet werden. Um Abhörversuche durch Bastler zu erschweren, sollten die Karten im Betrieb von allen unbewachten Terminals „verschluckt" werden, um abzusichern, dass keine an Drähten angeschlossene Karten gebraucht werden können.

Wird jedoch das Abhören technisch durchführbar, so ist für den Kryptanalytiker die Voraussetzung für den bekannten Klartext-Zugang gegeben. Auch wenn das Abhören unmöglich wäre, ist die Annahme nicht unrealistisch, dass der Kryptanalytiker eine eigene Karte/Terminal-Schnittstelle konstruieren könnte. Er könnte dann die Karte wiederholten Aufforderungen aussetzen und echte Antworten bekommen. Deshalb muss mit der Möglichkeit eines gewählten Klartext-Zugangs gerechnet werden, ob das Abhören wahrscheinlich ist oder nicht. Offensichtlich sollten die robusten Konzeptspezifikationen des DES-Verfahrens hier angewendet werden [13]. Im speziellen müssen die Nachrichtenblöcke lang genug sein, damit die Zusammenstellung einer adäquaten Tabelle von Klartext/Geheimtext-Paaren nicht durchführbar wird. Aus dem gleichen Grunde ist es erforderlich, dass die Aufforderungen unberechenbar sind. Bei einer Blocklänge von 64 Bit ist die Anzahl möglicher Aufforderungen ungefähr 1.8×10^{19}. Was bedeutet dies in der Praxis? Vorausgesetzt, dass die Anwortzeit der Karte für jeden Aufforderung/Rückmeldung-Zyklus 1 Mikrosekunde beträgt, würde der Kryptanalytiker gegen 580 000 Jahre benötigen, um die entsprechende Klartext/Geheimtext-Tabelle zusammenzustellen!

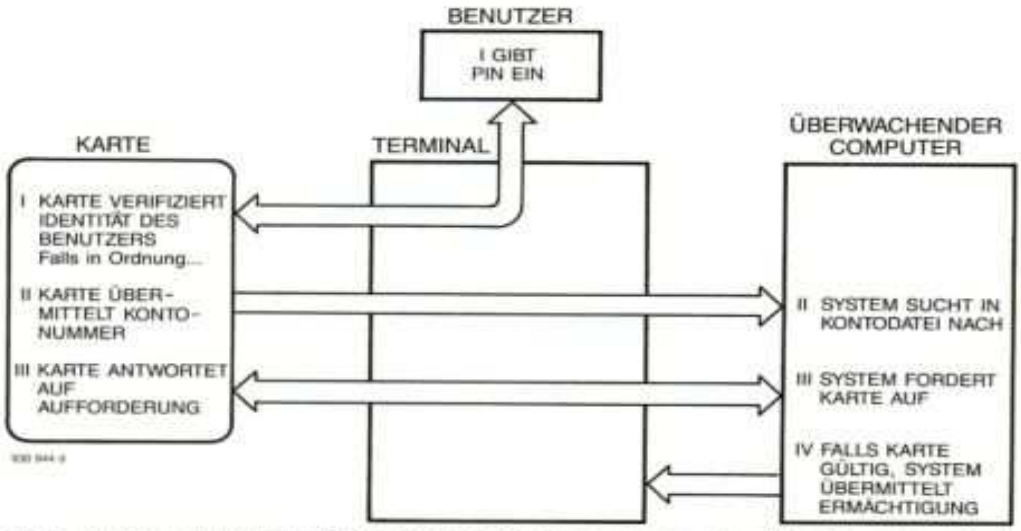

Bild 18 Beispiel des persönlichen Gebrauchs einer Mikroprozessorkarte an einem Online-Terminal (vereinfachtes Schema):
Im Schritt I wird die Identität des Karteninhabers von der Karte verifiziert. Im Schritt II wird die Identität der Karte an das System übermittelt. Im Schritt III prüft das System die Echtheit (und Identität) der Karte, bevor es im Schritt IV die Befugnis erteilt, die Transaktion durchzuführen.

Welche zusätzlichen konstruktiven Ideen können eingesetzt werden, um eine solche Kryptanalyse zu erschweren? Eine Möglichkeit ist, die maximale Wiederholungsrate elektronischer Anfragen zu begrenzen. Vorausgesetzt, dass die verwendete Mikroelektronik so konzipiert ist, dass sie eine wesentliche Erhöhung der externen Clockfrequenz nicht zulässt, kann eine Mindestzeitverzögerung von z.B. $^1/_{10}$ Sekunde zwischen Authentizitätskontrollen in die Karte einprogrammiert werden, ohne dass ihr normaler Betrieb merklich gestört wird. Die Zusammenstellung einer vollständigen Tabelle von 32 Bit Klartext/Geheimtext-Paaren braucht nur ungefähr 72 Minuten bei einer Wiederholungsrate von 1 Mikrosekunde. Beim Einbau einer Verzögerung von $^1/_{10}$ Sekunde wäre der Aufwand des Kryptanalytikers für die gleiche Aufgabe 13,6 Jahre! Eine zweite Möglichkeit, auf die in der Folge weiter ein-

gegangen wird, ist die Forderung, dass die Karte erst durch ein Passwort aktiviert wird.

Zusammenfassend bieten also elektronische Karten ein sinnvolles, verifizierbares Echtheitsmerkmal an unter der Voraussetzung, dass „Intelligenz" in Form einer Hardware-Logik oder eines Mikroprozessors in das Kartenkonzept eingebaut wird.

4. Fähigkeiten intelligenter Karten

Zwei Feststellungen über Mikroprozessoren sind für mögliche Anwendungen wegweisend. Erstens können die Rollen in den bereits beschriebenen kryptographischen Authentifizierungsvorgängen ohne weiteres ausgetauscht werden! Mit anderen Worten, eine Mikroprozessorkarte ist fähig, die Authentizität ihres Kommunikationspartners, wer oder was sich auch immer auf der anderen Seite der Karte/Terminal-Schnittstelle befindet, zu verifizieren. Zweitens können kryptographische Methoden verwendet werden (und werden es auch), um für die Authentizität und Geheimhaltung der Kommunikationen zwischen Benutzern in einer Netzwerkumgebung zu sorgen, in der auf Anlagen nicht verzichtet werden kann, deren Sicherheit gegen das Abhören nicht gewährt werden kann (die Bank-Telexmeldungen sind nur ein Beispiel). Auf gleiche Art und Weise kann die intelligente Karte das Lesegerät effektiv umgehen und private Kommunikationsverbindungen mit anderen Einheiten des Kartensystems herstellen, obwohl sie am Lesegerät angeschlossen werden muss.

Ehe auf die Verwendung intelligenter Karten für Zahlungs- und Zutrittszwecke weiter eingegangen wird, muss auch die potentielle Möglichkeit, sie für telematische Dienstleistungen einzusetzen kurz erwähnt werden. Für den Zugriff z.B. zu Bildschirmtext-Dienstleistungen stehen die gleichen Methoden zur Verfügung, die für allgemeinere Zahlungssysteme verwendet werden. Zusätzlich kann jedoch die Intelligenz der Karte für eine kritische Phase der Signalverarbeitung selbst eingesetzt werden. Folglich würde die Karte als eine Art elektronischer Schlüssel funktionieren, der für den einwandfreien Betrieb des Bildschirms unentbehrlich ist. Natürlich ist letzterer Betriebsmodus durch die verfügbare Geschwindigkeit und rechnerische Leistungsfähigkeit des Mikroprozessors begrenzt (für weitere Details siehe [20,21,22]).

Beim Konzipieren eines Mikroprozessorkartensystems steht man einer wahrhaften Pandorabüchse möglicher Sicherheitskontrollen gegenüber, die eventuell einzubeziehen sind. Das Kartenlesegerät kann die Echtheit einer Karte kontrollieren wie auch die Karte die Echtheit eines Endgeräts kontrollieren kann. In einem Onlinesystem kann die überwachende Zentrale Karten oder Terminals kontrollieren, so wie diese die Authentizität der Zentrale prüfen können. Gehört ein abgetrenntes Anwendungsmodul (z.B. ferngesteuertes Türschloss, Stromversorgungsschalter usw.) zum System, kann dieses ebenfalls die Zentrale, das Terminal oder die Karte kontrollieren respektive von diesen kontrolliert werden. In den meisten gegenwärtigen Systemen wird die Identität entweder vom Terminal oder von der Zentrale verifiziert – in der Tat kann die intelligente Karte das auch! Um die Palette theoretischer Möglichkeiten zu vervollständigen, sollte die Möglichkeit erwähnt werden, dass der Karteninhaber die Echtheit der oben erwähnten Komponenten zu bestätigen wünschte. So weit hergeholt dies auf den ersten Blick erscheinen mag, stellt es sich heraus, dass das Fehlen einer dieser Möglichkeiten eine denkbare Sicherheitslücke in gegenwärtigen Systemen für die bargeldlose Zahlung mit Mikroprozessorkarten darstellt. Bevor allgemeinere Möglichkeiten behandelt werden, sollte auch auf die neuartige Vorstellung, dass die Karte ihren Benutzer kontrolliert, eingegangen werden.

Liebhaber von Wildwestgeschichten nach der Hollywoodmanier können sich zweifellos an jene legendären Helden mit ihren ebenso legendären Pferden erinnern. Diese schnellen, kräftigen und edlen Pferde haben keinem anderen als ihrem berechtigten Reiter gestattet, sie zu reiten. Das elektronische Ebenbild des Einmannpferdes wird in Form der Mikroprozessorkarten, die jetzt in einigen Bankkartensystem-Prototypen im Einsatz sind, angeboten. Für jede Transaktion muss zuerst der Karte der PIN-Code ihres Inhabers zugeführt werden, ehe sie weitere Beweise für ihre Echtheit vorlegt. Ferner werden drei aufeinander folgende falsche Passwörter die Karte vor weiterer Benutzung sperren, bis sie an der Kartenausgabestelle der Bank neu aktiviert wird. Symbolisch funktioniert diese Karte wie ein mit einer Kombination versehener Schlüssel. Damit der Schlüssel das Schloss überhaupt öffnen kann, muss zuerst die richtige Kombination gewählt werden (*Bild 16*). Die weiteren Folgen dieser Sicherheitsmassnahme werden später behandelt, die folgenden drei daraus resultierenden Konsequenzen sind an dieser Stelle jedoch erwähnenswert. Erstens, falls Einträge über versuchte Kartenzugriffe im nichtflüchtigen Speicher nachgeführt werden, wird es möglich, die Karte nach einer *Anhäufung* von drei Fehlversuchen zu sperren. Es wird somit einem Dieb verunmöglicht, viele Passwörter auszuprobieren, indem er pro Terminal nur zwei Versuche auf einmal macht. Zweitens, falls die Karte persönliche Informationen für den Inhaber wie z.B. sein gegenwärtiges Bankkontoguthaben usw. trägt, ist die Vertraulichkeit dieser Daten gesichert. Drittens werden Versuche, solche Karten mittels einer gebastelten Karte/Lesegerät-Schnittstelle auszufragen, erschwert. Obwohl persönliche Indentifikationsnummern hier zur Diskussion stehen, kann die Idee einer Passwortkontrolle mit vorgesehener Sperrungsmöglichkeit auch auf unpersönliche Karten angewendet werden. Sie können nämlich vom Terminal ein Systempasswort verlangen, um aktiviert zu werden.

Ein Beispiel eines Authentifizierungsprotokolls, wie es für ein in der Literatur beschriebenes Onlinesystems mit Mikroprozessorkarten verwendet wird, ist in den *Bildern 17 & 18* dargestellt. Bild 17 dient zur

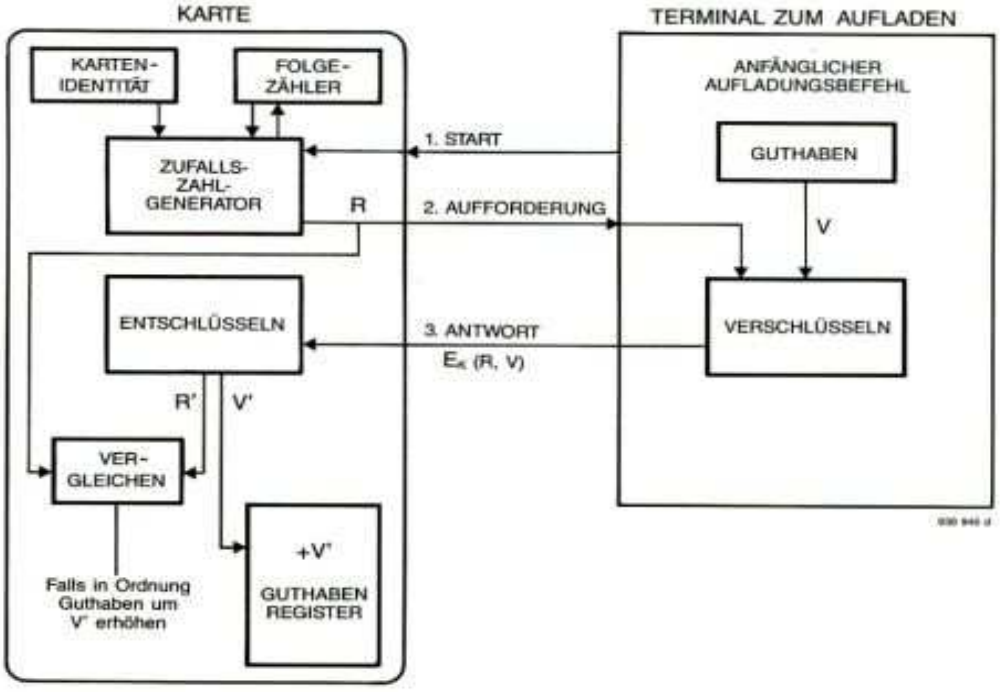

Bild 19 Das Aufladen einer entwertbaren Mikroprozessorkarte:
Im Schritt 1 gibt das Terminal der Karte ein Startzeichen, um den Aufladungsvorgang auszulösen. Im Schritt 2 fordert die Karte das Terminal mit einer Zufallszahl auf, sich auszuweisen. Falls die verschlüsselte Antwort vom Terminal die richtige ist, erhöht die Karte im Schritt 3 ihr Kreditregister um den erforderlichen Betrag.

Erläuterung der detaillierten Schritte, während Bild 18 das entsprechende Grundkonzept darstellt. Die Karte wird aktiviert, sobald sie den richtigen PIN-Code über eine Terminaltastatur bekommt. Anschliessend sendet sie die Kontonummer des Karteninhabers an das zentrale überwachende System. Das System prüft die Karte *direkt* mittels eines Aufforderung/Antwort-Protokolls. Der sogenannte Authentifizierungscode oder Geheimcode ist einem kryptographischen Schlüssel äquivalent, den das System in einer zentralen Datei nachsucht. Besteht die Karte die Echtheitsprüfung, so gibt das System dem Kartenlesegerät grünes Licht. Dieses Schema beinhaltet zwei der oben erwähnten neuartigen Merkmale. Erstens wurde die Verantwortung für die Verifizierung der Identität des Karteninhabers vom Terminal (oder System) an die Karte selbst übertragen. Zweitens wurde die Verantwortung für die Echtheitsprüfung der Karte vom Kartenlesegerät an das System übertragen. Das Terminal wurde jeglicher Verantwortung für den sicheren Systembetrieb enthoben!

An dieser Stelle muss die Sicherheitsfrage nochmals betrachtet werden. Bei den meisten Systemkonzepten wird die stillschweigende Annahme gemacht, dass eine allfällige Täuschung die Karte, den Benutzer oder beide betreffen kann, aber dass die Integrität von Terminals usw. als selbstverständlich betrachtet werden darf. Aber welche Komponenten eines Systems sind in Wirklichkeit zuverlässig? Hier muss ein wesentlicher Unterschied zwischen Online- und Offlinesystemen gemacht werden. In einem Offlinesystem fällt es notgedrungen den Terminals zu, die Echtheit der Karten zu kontrollieren.

Unter welchen Umständen ist an der Authentizität des Endgeräts zu zweifeln? Die Antwort lautet: wenn sich jemand durch ein falsches Terminal bereichern kann. Zum Beispiel kann durch Aufstellen eines falschen Terminals zum Entwerten vorbezahlter Wertkarten niemand profitieren. Handelt es sich jedoch um persönliche Karten, wäre ein möglicher Beweggrund für das Aufstellen eines falschen Kartenlesegeräts, *Informationen* wie z.B. PIN-Codes sowie Kartendaten vom nichtsahnenden Kartenbenutzer zu erlangen. In dieser Situation erweisen sich Magnetkarten ohne weitere besondere, unverfälschbare Merkmale wie z.B. optische Mikrostrukturen als ausgesprochen gefährdet. Ein anderer Beweggrund für die Manipulation von Terminals kann entstehen, wenn sie dafür verwendet werden, um Kredite für jemand anderen als den Systembetreiber einzunehmen. Dies betrifft Kreditkarten- bzw. direkte Debitkartensysteme, die *Endgeräte für die bargeldlose Zahlung*, sogenannte POS-Terminals („points-of-sales"), verwenden.

Da in POS-Systemen revisionspflichtige Kontos geführt werden, ist langfristiger, eklatanter Betrug durch an und für sich legitime Händler kaum zu erwarten. Ist trotz der hohen Kommunikationskosten ein Echtzeit-Onlinesystem vorhanden, ist es sinnvoll, wenn die zentrale Buchhaltungsstelle die Authentizität und den Status eines Kontokunden direkt verifiziert und anschliessend dem Händler gegebenenfalls sofort einen Kredit gutschreibt.

Nimmt man jedoch diskussionshalber an, dass es Betrüger gibt, die jegliche Möglichkeit zum Betrug wahrnehmen, in was für einen Betrug würde dann ein POS-Terminal verwickelt? Ein echtes Lesegerät kann modifiziert werden oder eine vollständige Nachahmung, die wie das Original funktioniert und aussieht, kann gebaut werden. Wie bereits erwähnt, kann ein solches Gerät eingesetzt werden, um Kundenkontodaten und entsprechende PIN-Codes zu erfahren, mit der Absicht, Karten nachträglich zu fälschen. Im anderen Falle kann ein unehrlicher Händler diese Information verwenden, um fiktive Käufe zu simulieren oder den Wert wirklicher Transaktionen zu seinen Gunsten zu modifizieren.

Wie ist die Täuschung durch Terminals zu verhindern, und im speziellen wie lassen sich die verschiedenen Kartentypen miteinander vergleichen? Im Falle eines Scheinterminals für die Aufzeichnung von Konto- und PIN-Daten sollten die Karten mindestens einige Daten enthalten, die nicht auf andere Karten kopiert werden können. Für diesen Zweck ist die Landis & Gyr-optisch codierte Karte geeignet. Vorstellbar ist auch eine Karte, die einen Magnetstreifen zuzüglich optisch codierte Informationen enthält, sofern die optischen Daten *individuell codiert* und kryptographisch mit allfälligen kritischen Daten auf der Magnetpiste *korreliert* sind. Mikroprozessorkarten sind auch geeignet, vorausgesetzt dass persönliche Daten nicht modifiziert werden können, nachdem sie einmal eingegeben wurden. Die Mikroprozessorkarte kann noch einen Schritt weiter gehen, und die Echtheit des Terminals kontrollieren, bevor sie Informationen über das Konto des Benutzers abgibt. Wozu die gegenwärtige intelligente Karte jedoch *nicht* fähig ist, ist ihren Inhaber vor der Eingabe seines PIN-Codes zu warnen, falls er an ein zweifelhaftes Terminal gerät.

Um die Simulation oder Manipulation einer Transaktion zu verhindern, wird das überwachende System notwendigerweise daran beteiligt. Grundsätzlich muss das System kontrollieren, ob ein legitimer Karteninhaber die Transaktion auch tatsächlich genehmigt hat. Falls ausserdem das Terminal verdächtig ist, muss die Transaktion selbst in bezug auf den Betrag und die Identität des Kreditbegünstigten kontrolliert werden. Das System kann die Identität des Terminals mittels eines Aufforderung/Antwort-Protokolls, das einen kryptographischen, dem Terminal eigenen Schlüssel verwendet, verifizieren. Wie kontrolliert man jedoch den Betrag der Transaktion? Werden in einem System keine Buchhaltungseinträge auf der Karte gemacht, so kann dem Kunden ein Papierbeleg gegeben werden, was eine nachträgliche Gegenkontrolle mit den zentralen Kontodaten ermöglicht. Im Falle der Mikroprozessorkarte ist es möglich, für die Übereinstimmung zwischen den Einträgen auf der Karte und jenen an der zentralen Buchhaltung zu sorgen. Das Terminal kann nämlich die Kaufsumme sowohl auf die Karte wie auch auf das System übertragen und die Karte kann die verschlüsselten Transaktionsdetails in ihrer Antwort auf eine Aufforderung des Systems einschliessen oder umgekehrt. Was die gegenwärtige intelligente Karte *nicht* verhindern kann, ist jedoch der Einsatz eines Terminals, bei dem die Tastatur und Anzeige einen Betrag angeben aber für diesen einen höheren Betrag in den Kommunikationen mit der Karte und Zentrale einsetzen! Keine gegenwärtig vorhandene Karte kann diese besondere Art von Betrug verhindern!

Folglich ist es offensichtlich, dass entweder Entwickler eines Onlinesystems die Integrität der verwendeten Terminals garantieren muss oder dass neue Eigenschaften der intelligenten Karte erforderlich sind. Ist die erste Alternative machbar, so sind die besonderen Fähigkeiten der Mikroprozessorkarte weitgehend überflüssig. Etablierte Technologien wie die Landis & Gyr-optisch codierte Karte sind in diesem Falle mindestens so sicher und zudem wirtschaftlicher. Kann die Zuverlässigkeit des Terminals nicht vorausgesetzt werden, so entsteht die Sicherheitslücke durch das Fehlen einer direkten *Karte/Benutzer-Schnittstelle*. Falls an den Karteninhaber keine sichtbare Quittung seines Kaufs abgegeben wird, sollte die Mikroprozessorkarte die Transaktion authentifizieren, bevor sie dieselbe in den Speicher einträgt. Die Mikroprozessorkarte ist wohl in der Lage, die Richtigkeit des Betrags zu prüfen – sie kann das Terminal auffordern und eine verschlüsselte Antwort einschliesslich Transaktionsdetails verlangen. Aber wie weiss der Kunde *was* die Karte genehmigt hat? Aus dieser Sicht ist die existierende „intelligente" Karte „taub" und „stumm". Es würde eine direkte Karten/Karteninhaber-Schnittstelle wie z.B. eine Flüssigkristall-Anzeige benötigt, um den Kaufbetrag, der durch die Karte entschlüsselt wurde, anzuzeigen.

Im gleichen Sinne könnte eine Karte mit einer einfachen Tastatur versehen werden. Dies würde die Vertraulichkeit des PIN-Codes schützen, da die am Terminal angeschlossene Tastatur umgangen werden könnte. Würde überdies die Karte mit einer Batterie versehen, so könnte die Sicherheit der kryptographischen Schlüssel und Algorithmen durch deren Aufbewahrung in einem verlierbaren Speicher wesentlich erhöht werden. Eine sichere Karte mit diesen Verfeinerungen könnte treffenderweise als die „superkluge" Karte bezeichnet werden.

Um die Sicherheit des Gesamtsystems zu bewerten, muss die Möglichkeit, die überwachende Zentrale selbst zu simulieren, in Betracht gezogen werden. Es ist wichtig in einem POS-Onlinesystem, dass der Händler genau weiss, ob das überwachende System eine Transaktion genehmigt hat. Deshalb muss die Genehmigung selbst authentifiziert werden – d.h. das Endgerät muss das System auffordern und die Genehmigung in Form einer richtig chiffrierten Antwort bekommen. Sonst besteht das Risiko, dass mit einer für diesen Zweck konstruierten Elektronik das Terminal zu der Annahme verleitet wird, dass die Transaktion genehmigt wurde, während in Wirklichkeit das Gegenteil zutrifft.

Die Aufgabe, die Echtheit des Kartenlesegeräts (oder sogar des Systems) zu prüfen, stellt an die Mikroprozessorkarte gewisse technische Forderungen. Sie muss Meldungen verschlüsseln können und zudem unvorhersehbare Zufalls- oder Pseudozufallsbitfolgen erzeugen können. Im Hinblick auf die Grenzen des Kartenspeichers wäre eine sinnvolle Möglichkeit, individuelle Kartendaten zusammen mit dem gegenwärtigen Zustand eines Einwegsequenzzählers zu chiffrieren. Die Nichtlinearität der Verschlüsselung sorgt für die Pseudozufälligkeit der Folge so erzeugter Zufallszahlen, und die Einbeziehung individueller Kartendaten bei diesem Vorgang sorgt dafür, dass eine Folge von Zufallszahlen von der einen Karte keine nützliche Informationen über die von einer anderen erzeugten Zufallszahlen enthält. Die Verwendung eines Sequenzzählers, der nur in einer Richtung zählt, verhindert die Wiederholung einer Folge von Zufallszahlen, die sonst aus einer möglichen Zurücksetzung des Zählers resultieren könnte.

Bietet die Mikroprozessorkarte gegenwärtig die einzige Möglichkeit, für die Systemsicherheit bei unabgesicherten Terminals zu sorgen? Können „passive" Karten in POS-Systemen eingesetzt werden? Obwohl die besonderen Fähigkeiten der Mikroprozessorkarte bei dieser Sicherheitsproblematik eine bestechend elegante Lösung bieten, stellt die heutige intelligente Karte keinewegs die einzige Lösung dar. Eine sinnvolle Alternative wird durch die Verbindung konventioneller, sicherer Kartentechnologie mit den in diesem Artikel besprochenen krypographischen Authentifizierungsprinzipien geboten. Ein versiegeltes Kartenlesemodul, das mindestens mit einem Mikroprozessor versehen ist, welcher kryptographische Fähigkeiten aufweist, kann in jedem Terminal eingebaut werden (*Bild 19*). Das Modul wird die Echtheit der Karte direkt prüfen und Kontoinformationen des Inhabers ablesen. Es wird seine kryptographische Einrichtung verwenden, um diese Daten in Antwort auf eine Anfrage des Systems zu authentifizieren. Dieses Konzept ermöglicht den Gebrauch komplexerer kryptographischer Protokolle als diejenigen, die durch die Mikroprozessorkarte angeboten werden. Überdies bietet das Modul potentiell verbesserte physische Sicherheit an, weil es mit flüchtigen an der Speisung angeschlossenen Speichern versehen werden kann, so dass kryptographische Algorithmen und Schlüssel beim Öffnen des Moduls gelöscht werden. Falls erforderlich, kann die Verifizierung des PIN-Codes im Modul durchgeführt werden.

Im wesentlichen verlangt dieses Konzept ausser der physischen Sicherheit des Moduls, dass die Karten nicht *kopiert werden können*. Wie bereits erwähnt, kann eine Karte, welche mit Landis & Gyr-optisch codierten Merkmalen versehen ist, die notwendige Sicherheit anbieten. Die kryptographische Einheit wird benötigt, um auszuschliessen, dass Informationen über Karten durch ein falsches oder manipuliertes Terminal aufgezeichnet und, mit der Absicht, fiktive Transaktionen dem System als echt vorzutäuschen, nachträglich an das System abgespielt werden. Ob diese kryptographische Einrichtung sich innerhalb der Karte oder in einem versiegelten Modul im Kartenlesegerät befindet, ändert wenig am Konzept. Es ist jedoch von wirtschaftlichem Vorteil, die kryptographischen Anlagen in Tausenden von POS-Terminals zu konzentrieren anstatt in Millionen von Karten zu verteilen.

5. Entwertbare und aufwertbare intelligente Karten?

Wie erwähnt kann die Echtheit intelligenter Karten kontrolliert werden, indem man die Karten unvorhersehbare, genügend lange digitale Aufforderungen verschlüsseln lässt. Solche Karten können auch als entwertbare Karten verwendet werden, wenn eines der Funktionsprinzipien des PHONOCARD-Systems übernommen wird, nämlich wenn die Restwertdaten selbst geprüft werden und jeder Entwertungsvorgang bestätigt wird (*Bild 20*). Dies deutet auf einen Entwertungsvorgang hin, bei dem das Terminal der Karte den geeigneten Befehlscode, gefolgt von einer Zufallszahl, sendet. Es wird dann von der Karte verlangt, dass sie diese Zufallszahl zusammen mit dem neuen Restwert als Geheimtext zurücksendet.

Die Aufwertung von Karten stellt bekanntlich ein heikles Sicherheitsproblem dar. Gerade in dieser Situation kann die Fähigkeit der intelligenten Karte, ihre Umgebung zu prüfen, vorteilhaft eingesetzt werden. Um die betrügerische Aufwertung von Karten auszuschliessen, muss die Echtheit legitimer Aufwertungsbefehle einwandfrei

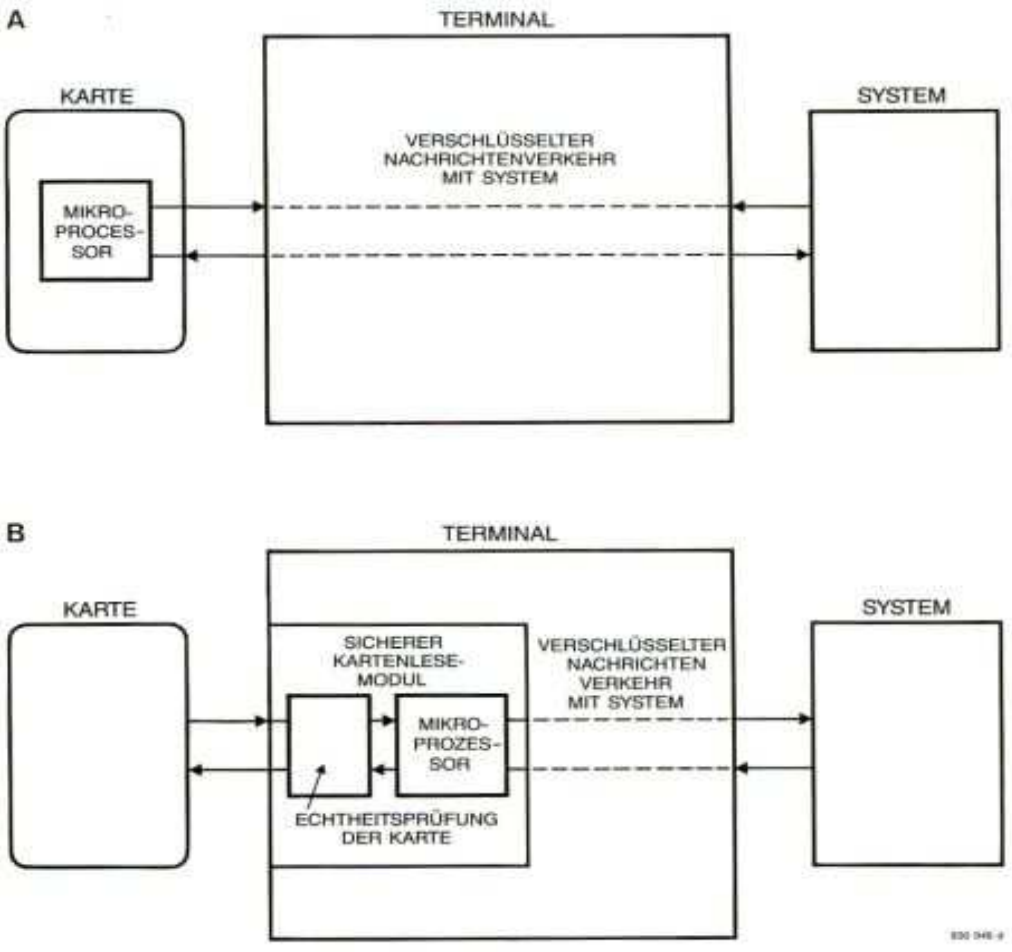

Bild 20 Zwei Lösungen bei Online-Systemen mit unsicheren Terminals:
A) Den Mikroprozessor in der *Karte* einbauen – die Karte wird vom System geprüft
B) Den Mikroprozessor in einem versiegelten *Kartenlesemodul* einbauen – der Kartenlesemodul wird vom System geprüft

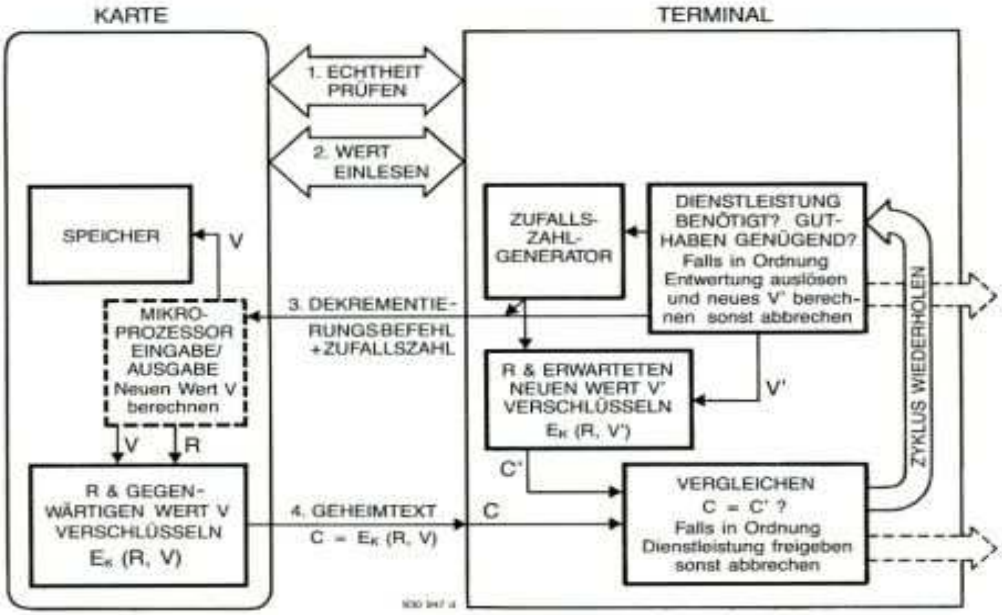

Bild 21 Beispiel eines Entwertungszyklus in einer Mikroprozessorkarte:
Jede Entwertung der Karte wird mit Hilfe eines kryptographischen Authentifizierungsprotokolls geprüft.

nachgewiesen werden. Folglich wird eine Aufforderung an das aufwertende Terminal benötigt, dessen Antwort gegebenenfalls Informationen über den relevanten Betrag enthalten kann. Im Prinzip gestattet dieses Protokoll die Verwendung einer Karte mit einem völlig reversiblen Speicher als entwertbare Karte. Die Karte verifiziert, ob die Instruktionen, die sie bekommt, von berechtigten Quellen kommen. Die kritische Forderung, welche die Sicherheit betrifft, ist, dass Einzelheiten über die Chiffrieralgorithmen, Zufallszahlgenerator und verschiedene verwendete Schlüssel *nicht aus der Karte extrahiert werden können.*

Für welche besonderen Zwecke kann die Public-Key-Kryptographie nun eingesetzt werden? Hier wird zusammenfassend darauf hingewiesen, dass Sicherheitsvorgänge in Kartensystemen primär Authentifizierungsprozeduren sind, und dass Public-Key-Methoden von besonderem Interesse sind, falls ein Schlüssel gefährdet werden könnte. Weil der schwächste Schlüsselträger wahrscheinlich die Karte ist, sollte sie einen öffentlichen Schlüssel enthalten. Mit diesem kann sie z.B. ein Endgerät prüfen. Ein Public-Key-Algorithmus kann also vorteilhaft z.B. für die Aufwertung von Wertkarten eingesetzt werden. Um die von Public-Key-Algorithmen angebotene Sicherheit optimal auszunützen zu können, müssten die Aufforderungen durch einen *zuverlässigen Generator echter Zufallszahlen* erzeugt werden. Im Hinblick auf die Abhängigkeit der Karte von einer externen Speisung, wird hier offensichtlich sehr viel verlangt! Wird ein anderer, auf individuelle Kartendaten basierender Pseudozufallszahlengenerator verwendet, so wird die Preisgabe der Authentifizierungsprozeduren der einen Karte es einem aktiven Horcher nicht ermöglichen, sich als ein legitimes Terminal beim Umgang mit einer anderen Karte auszugeben. Folglich bietet die Public-Key-Kryptographie die Möglichkeit, die Sicherheit bei der Eintragung von Kreditkarten auf die Karten zu erhöhen, sofern die einzelnen Karten so konzipiert sind, dass sie individuelle Authentifizierungsaufforderungen erzeugen können (*Bild 21*).

In der Praxis ist jedoch die Public-Key-Kryptographie bei Anwendungen von Mikroprozessorkarten von begrenztem Wert wegen der verhältnismässig hohen *rechnerischen Komplexität,* die für die Einhaltung des vorgeschriebenen Sicherheitsniveaus erforderlich ist. Beim RSA-Algorithmus wird die Integerarithmetik modulo Zahlen in der Grössenordnung von ungefähr 200 Dezimalstellen empfohlen. In anderen Worten muss der Mikroprozessor fähig sein, arithmetische Operationen mit ungefähr 700-Bit Zahlen vorzunehmen! Wahrscheinlich muss auf sprunghafte Fortschritte im Chip-Entwurf oder einfachere (aber immer noch sichere) Public-Key-Algorithmen gewartet werden, bevor Public-Key-Methoden in intelligenten Karten wirtschaftlich eingesetzt werden können.

In jedem Fall gilt die Regel, dass die Sicherheit sowohl der Authentifizierung von Karten wie auch der Aufwertung derselben von der vorausgesetzten physischen Integrität der in der Karte eingebauten Mikroelektronik abhängt, ob die Public-Key-Kryptographie verwendbar ist oder nicht.

Schlussbetrachtungen

Voraussetzung für die Sicherheit in Kartensystemen ist die eindeutige Erkennung von echten Karten, die Überprüfung allfälliger darauf vorhandener persönlicher Daten oder Wertangaben, und die technische Undurchführbarkeit des unbefugten Manipulierens solcher Daten. Bei Offlinesystemen oder bei Onlinesystemen, deren Kartenlesegeräte als gesichert gelten, kann man behaupten, dass ein System, das die optische Codierungstechnologie von Landis & Gyr verwendet, die wirtschaftlichste Lösung darstellt, die den genannten Forderungen vollständig genügt.

Elektronische Karten, die in der Lage sind, genügend komplexe kryptographische Operationen auszuführen, können auch so gestaltet werden, dass sie die oben erwähnten Sicherheitsspezifikationen erfüllen. Hinreichende *kryptographische* Sicherheit wird gewährleistet, falls Aufforderung/Antwort-Prüfverfahren verwendet werden, bei denen die Telegramm- und Schlüssellängen mindestens in der Grössenordnung von 64 Bit liegen. Die *allgemeine* Sicherheit bedingt den Gebrauch von VLSI mikroelektronischen Komponenten, die gegen allfällige Versuche, die abgespeicherten geheimen Schlüssel und Algorithem herauszulesen, *physikalisch* abgesichert sind.

Es ist zwar möglich, Mikroprozessorkarten als unpersönliche Wertkarten einzusetzen. Für diesen Zweck jedoch bietet z.B. das PHONOCARD-System eine Alternative, die mindestens so sicher aber bedeutend wirtschaftlicher ist. Obwohl das Wiederaufladen verbrauchter Mikroprozessorkarten technisch machbar wäre, ist es sehr fraglich, ob die damit verbundenen administrativen Unkosten ein solches Verfahren rechtfertigen würden. Zudem würden die Anlagen für das Wiederaufladen der verbrauchten Karten selbst grosse Anforderungen an die Sicherheit stellen (und das unabhängig von der verwendeten Kartenart).

Die besonderen Fähigkeiten der intelligenten Karte erscheinen für Onlinesysteme vorteilhaft, bei denen die *Integrität* der verwendeten *Kartenlesegeräte* nicht gewährleistet werden kann, wie zum Beispiel Terminals für die bargeldlose Zahlung („point of sales"). Die Mikroprozessorkarte ist in der Lage, die Echtheit ihrer Kommunikationspartner sowie die Identität ihres Inhabers zu prüfen.

Eine gleichwertige Alternative in dieser Situation wäre, die Terminals mit versiegelten, sicheren Lesemodulen auszurüsten, die fehlergeschützte kryptographische Komponenten verwenden. Hinreichende Sicherheit könnte dann mit „konventionellen" Karten, bei denen das Kopieren oder die Manipulation von Daten unmöglich ist, wie z.B. die Landis & Gyr-optisch codierte Karte, gewährleistet werden.

Ferner ist die durch die heutigen Mikroprozessorkarten angebotene Sicherheit nicht

vollständig. Im speziellen fehlt die direkte Kommunikation zwischen der intelligenten Karte und ihrem Inhaber, was dazu führen könnte, dass ein allfälliger Betrug durch ein falsches oder manipuliertes Kartenlesegerät unbemerkt blieb. Die intelligente Karte der Zukunft sollte womöglich mit einer Anzeige und einer Tastatur ausgerüstet sein. Eine solche „superkluge" Karte würde eher versprechen, alle erwünschten Sicherheitsanforderungen zu erfüllen.

Autoren: Andrew S. Glass
LGZ Landis & Gyr Zug AG
CH-6301 Zug (Schweiz)

James L. Massey
Eidgenössische Technische Hochschule
CH-8092 Zürich (Schweiz)

Übersetzer: A. & K. Glass, T. Schaub
LGZ Landis & Gyr Zug AG

Bibliographie

[1] Moreno, R.: Un support individuel d'information inviolable, Informatique, 1979 No. 129

[2] Weinstein, S.B: Smart credit cards: the answer to cashless shopping, IEEE Spectrum, 21(1984)2, S. 43–49

[3] Greenaway, D.L.: Karten und Kartenleser für Geldersatz- und Zutrittskontrollsysteme, Landis & Gyr-Mitteilungen 27(1980)1, S. 21–26

[4] Wirth, U.: Zutrittskontrollsystem ID2000, Landis & Gyr-Mitteilungen 27(1980)1, S. 47–52

[5] Wiblé, P.: PHONOCARD – eine Telephonstation mit vorbezahlten Karten, Landis & Gyr-Mitteilungen 27(1980)1, S. 40–46

[6] Dändliker, G.: Anforderungen, Probleme und neue Konzepte öffentlicher Fernsprecher, Landis & Gyr-Mitteilungen 30(1983)1, S. 2–6

[7] Moser, J.-F.: Die Plastikkarte als Informationsträger für Geldersatz- und Ausweisapplikationen, Landis & Gyr-Mitteilungen 28(1981)1, S. 9–14

[8] Lienhard, H.: Die optisch codierte Karte: System- und Sicherheitsaspekte, Landis & Gyr-Mitteilungen 27(1980)1, S. 14–20

[9] Schalkwijk, J.P.M: An algorithm for source codes, I.E.E.E. Transactions on Information Theory, 1972 IT-18, S. 395–399

[10] Cover, T.M.: Enumerative source coding, I.E.E.E. Transactions on Information Theory, 1973 IT-19, S. 73–77

[11] Massey, J.L.: Applied Digital Information Theory, Vorlesungsnotizen, Institut für Signal- und Informationsverarbeitung, Eidg. Technische Hochschule (ETH), Zürich, 1984

[12] Rejewski, M.: How Polish mathematicians deciphered the Enigma, Annals of the History of Computing, 3(1981), S. 213–234

[13] Data Encryption Standard, 1977, F.I.P.S. Publication 46, National Bureau of Standards, U.S. Dept. of Commerce

[14] Kahn, D.: The Codebreakers: the Story of Secret Writing, 1967, (McMillan, New York)

[15] Diffie, W.:, Hellman, M.: New directions in cryptography, I.E.E.E. Transactions on Information Theory, 1976, IT-22, S. 644–654

[16] Hellman, M.: The Mathematics of Public-Key Cryptography, Scientific American, 241(1979)2, S. 130–139 (8/79)

[17] Rivest, R., Shamir, A., Adleman, L.: On digitals signatures and public key-cryptosystems, Comm. of A.C.M., 21(1978), S. 120–126

[18] Hardy, G.H., Wright, E.M.: The Theory of Numbers, 4th Edn. (1960), Oxford U.P.

[19] Agnew, G.B.: Privacy and Secrecy in Computer Networks, Vorlesungsnotizen Institut für Signal- und Informationsverabeitung, Eidg. Technische Hochschule (ETH), Zürich, 1984

[20] Le Rest, D., Guillou, L.: Public Key Algorithms and Telematic Services, Conference proceedings, I.E.E.E. International Symposium on Information Theory, Les Arcs, France, June 21–25, 1982

[21] Lambert, C.: Radiodiffusion à accès sélectif, Conference proceedings, S.E.E./I.R.E.S.T. Colloque «La carte à mémoire», May 4–6, 1983

[22] Schröther, E.: Verschlüsselungsverfahren und Chipkarte erhöhen Btx-Sicherheit, Btx Praxis, (1984)8, S. 13–16

Sodeco-Saia AG
Grand Pré 70
CH-1211 GENF 16
Telefon 022-33 55 00
Telex 22 333

LANDIS & GYR

TID-CH 130 Gedruckt in der Schweiz 058604 Kdg