Karten und Kartenleser für Geldersatz- und Zutrittskontrollsysteme

DK: 681.131:336.7.002.69:535.411
351.755.6:535.411

D. L. Greenaway

Gegenstand dieses Artikels sind zwei Gruppen von neuen Produkten und die ihnen zugrunde liegende Technologie. Bei der ersten Gruppe handelt es sich um die Realisierung von Geldersatzsystemen, die mittels vorausbezahlter Karten betrieben werden. Als typisches Beispiel wird das System PHONOCARD beschrieben, das von der zum Landis & Gyr-Konzern gehörenden Gesellschaft Sodeco-Saia hergestellt wird. Die zweite Gruppe von Produkten betrifft die Herstellung von Identifizierungssystemen, die durch maschinell lesbare Karten betrieben werden. Als Beispiel dient hier das Kartenlesegerät ID 2000 für die Zutrittskontrolle, das bei Landis & Gyr in Zug hergestellt wird.

Bild 1 PHONOCARD-Station

1. Einleitung

Beide erwähnten Produkte beruhen auf einem gemeinsamen Konzept zur Verschlüsselung von Information mit höchsten Sicherheitsansprüchen. In Anbetracht dieser Sicherheitsansprüche ist es verständlicherweise unumgänglich, in den folgenden Abschnitten eine Reihe von spezifischen Einzelheiten mit Absicht auszulassen. Der Autor hofft, trotz dieser notwendigen Einschränkung einen interessanten Überblick über die Anwendung einer modernen Technologie auf ein Gebiet von zunehmender kommerzieller Bedeutung bieten zu können.

2. Anwendungen

Die Anwendungen lassen sich am besten in zwei Gruppen einteilen: einerseits in Geldersatzsysteme und andererseits in Identifizierungssysteme. Beide sind bestimmten Randbedingungen unterworfen, und zwar sowohl im Hinblick auf das benötigte Sicherheitskonzept als auch auf die wirtschaftliche Herstellung von Karte und Leseausrüstung. Daher werden die beiden Systemgruppen in den folgenden Abschnitten, wo nötig, getrennt behandelt.

Ein Beispiel für Anwendungen auf dem Gebiet des Geldersatzes ist das System PHONOCARD. Die PHONOCARD-Einheit ist ein vollwertiger Ersatz für die heute noch im öffentlichen Fernsprechverkehr gebräuchlichen Münzfernsprecher. Die in *Bild 1* gezeigte PHONOCARD-Station hat keinerlei Geld- oder Münzbehälter. Vielmehr akzeptiert sie eine vorausbezahlte Karte, die eine Anzahl Werteinheiten enthält. Diese Werteinheiten (von denen die einfachste Version der Karten bis zu 120 Stück enthält) entsprechen den Gebühreneinheiten des Telephonnetzes. Sie werden im Laufe des mit Hilfe

der Karte geführten Telefongesprächs entwertet, und zwar mit der Geschwindigkeit, die dem jeweiligen Tarif entspricht. Dabei handelt es sich um eine Einweg-Karte, die nicht wieder neu mit Werteinheiten versehen werden kann. Die Karte kann jedoch wiederholt für Orts- und Ferngespräche verwendet werden, bis alle ihre Werteinheiten verbraucht sind.

Die PHONOCARD-Station zeigt den Stand der noch auf der Karte verbliebenen Werteinheiten an. Überdies wird es Karten geben, bei denen der Stand jederzeit auf der Karte selbst sichtbar ist. Das System ist für den Benützer sehr bequem. Das gilt vor allem für Ferngespräche, bei denen die Bereithaltung des exakten Münzbetrages für die herkömmlichen Münzfernsprecher häufig ein Problem darstellt. Für den einzelnen Benützer bedeutet die Vorauszahlung keinen ins Gewicht fallenden finanziellen Verlust. Die gesamte Vorauszahlung für alle im Umlauf befindlichen Karten stellt hingegen für die Institution, die das System betreibt, einen beträchtlichen finanziellen Vorteil dar. Ferner spart diese Institution die Kosten, die das Einsammeln, Zählen und Eintauschen grosser Mengen von Münzen niedriger Wertstufen mit sich bringt. Man darf auch erwarten, dass das Fehlen von Münzen zu einem Rückgang der in manchen Ländern häufigen mutwilligen Zerstörung von Münzfernsprechern führt, ein Umstand, der die Betriebskosten stark beeinflussen kann.

Die vorausbezahlte Karte und der in der PHONOCARD-Station eingebaute Kartenleser lassen sich nicht nur für telephonische Zwecke verwenden, vielmehr können sie überall dort eingesetzt werden, wo Einnahmen durch Automaten kassiert werden müssen. Beispiele sind:

- der Benzinverkauf von nichtgewarteten Zapfsäulen,
- das Kassieren von Parkgebühren bei grossen Parkplätzen oder -häusern,
- die Bezahlung elektrischer Energie mit Hilfe eines mit dem Elektrizitätszähler verbundenen Kartenlesers,
- das Kassieren des Fahrpreises bei öffentlichen Transportunternehmungen.

Als konkretes Beispiel der verschiedenen Anwendungsmöglichkeiten wird gegenwärtig das System PHONOCARD in Belgien in öffentlichen Feldversuchen getestet, die unter Aufsicht der belgischen Telephongesellschaft RTT stattfinden. Der Beginn von Feldversuchen in einigen anderen Ländern, nämlich Frankreich, Österreich und der Schweiz, ist für 1980 geplant. Der Benzinverkauf mittels vorausbezahlter Karte wurde während des vergangenen Jahres intern bei Sodeco-Saia in Genf erprobt. An zwei Stellen der Zürcher Innenstadt ist die Einführung eines auf der Karte beruhenden Parksystems für das Frühjahr 1980 geplant.

Die zweite allgemeine Gruppe von Anwendungen betrifft die persönliche Identifizierung. Ein Vertreter davon ist das System ID 2000: Zutrittskontroll-Lesegerät und -karte.

In ihrer einfachsten Form funktionieren Lesegerät und Karte als ein hochentwickeltes Schlüsselsystem, das je nach der auf der Karte verschlüsselten Information den Zugang zu einer Anzahl von Räumen mit vorher bestimmten Zeit- und Zonenprioritäten ermöglicht. Die Lesegeräte können autonom betrieben werden oder können mit einer zentralen Datenverarbeitungseinheit verbunden werden, was den Einbau einer ganzen Reihe weiterer Eigenschaften erlaubt.

Der im *Bild 2* gezeigte einfache Kartenleser enthält keinen Transportmechanismus. Vielmehr wird die Karte von Hand eingeführt und durch einen Schlitz geschoben, um das Auslesen der (unsichtbaren) Informationen durch einen im Gerät befindlichen optischen Lesekopf zu ermöglichen. Die ausgegebenen Karten sind entweder neutral (für reine Zugangskontrollanwendungen) oder mit einer eingravierten Photographie des Benützers und weiterer graphischer Informationen zum Zwecke der visuellen Identifizierung versehen (z.B. als ein vom Benützer zu tragender Sichtausweis). Zutrittskontrollsystemen mit hoher Sicherheit, wie dem System ID 2000, fällt eine bedeutende Rolle in der ganzen Sicherheitsindustrie zu, bei der es sich, angesichts der unbeständigen heutigen Welt, um eine Branche mit dynamischem Wachstum handelt. Zur Zeit hat das System ID 2000 vor allem die Aufgabe, den Zugang zu gewissen Räumen und Geräten zu kontrollieren (z.B. Computer-Terminal). Für die Zukunft darf man eine Erweiterung auf das Gebiet der allgemeinen Identifizierung von Personen erwarten: von der Überwachung finanzieller Transaktionen bis zur Passkontrolle.

27 652

Bild 2 Kartenleser ID 2000

3. Physikalisch-technische Grundlagen

Sowohl bei Systemen vom Typ PHONOCARD als auch bei denjenigen vom Typ ID 2000 beruht die Verschlüsselung der Information auf holographischen Verfahren. Ein Hologramm ist die Aufzeichnung einer Interferenz zwischen zwei oder mehr miteinander kohärenten Feldern. Die spektakulären Eigenschaften der holographischen Aufzeichnung – nicht zuletzt die dreidimensionale Bildrekonstruktion – sind wohlbekannt. Solche dreidimensionale Hologramme weisen im allgemeinen eine äusserst hohe Dichte der gespeicherten Information (bis zu 10^6bits Bildinformation pro Quadratmillimeter) auf. Zudem zeichnen sie sich durch höchste räumliche Auflösung aus: die Bildinformation ist beispielsweise als räumliche Modulation des optischen Absorptionsvermögens aufgezeichnet, wobei Raumfrequenzen von 1000 Linien/mm oder mehr vorkommen. Angesichts der hohen Raumfrequenzen ist zur Aufzeichnung von Hologrammen eine sehr spezielle Technologie nötig, und schon diese Tatsache allein bedeutet Sicherheit z.B. gegen Fälschung. Diese hohe räumliche Auflösung wird beim Einsatz holographischer Techniken für unsere Kartensysteme tatsächlich ausgenutzt, aber im Hinblick auf die Erfordernisse eines maschinell lesbaren Systems ist der Informationsgehalt viel kleiner. Diese Reduktion des Informationsgehalts hat zwei wichtige Konsequenzen, die beide mit der wirtschaftlichen Herstellung eines funktionierenden Lesekanals für diese Art Information zu tun haben. Erstens wird für einen Lesekanal nur eine kleine Anzahl Detektoren benötigt. Eine grosse Anzahl Detektoren würde sofort zu einem Anstieg der Kosten des Lesegeräts führen. Zweitens braucht man wegen des geringen Informationsgehalts für die Rekonstruktion der holographischen Information keinen Laser mehr, sondern es genügt eine inkohärente Lichtquelle (z.B. eine lichtemittierende Diode).

Bei den hier beschriebenen Geldersatz- und Identifizierungssystemen wird ein holographisch aufgezeichne-

tes Muster bei der Kartenherstellung in der Kartenstruktur vergraben. Das Lesegerät ist mit einer Infrarotlichtquelle und mit einem optischen System ausgerüstet. Dieses fragt das vergrabene Muster ab und produziert in den Detektoren ein charakteristisches Signal, durch welches die Echtheit der Karte festgestellt wird. Bei einem Geldersatzsystem – z.B. PHONOCARD – enthält die Karte eine ganze Sequenz solcher Muster, und jedes Feld muss das richtige optische Signal hervorrufen. Die Entwertung wird thermisch durchgeführt, und zwar werden die Aufzeichnungen eine nach der andern mittels eines geheizten Löschkopfes zerstört. Der Löschkopf ist Bestandteil des Kartenlesers und wird durch die Zeitimpulse der Telephonlinie gesteuert. Das Löschen wird von einer charakteristischen Änderung der Detektorsignale begleitet und bietet somit eine weitere Kontrolle der Echtheit der Karte.

Bei Identifizierungssystemen – z.B. ID 2000 – enthält das Lesegerät keinen Löschkopf. Hingegen enthält die Karte eine verschlüsselte Folge von Mustern. Jedes Feld muss ein charakteristisches Signal in den Detektoren hervorrufen. Wenn die Karteninformation im Lesegerät abgetastet wird, erscheint eine spezifische Folge von Signalen, die mit der in der Karte gespeicherten digitalen Information (typisch 96 bits) verknüpft ist.

Es ist im allgemeinen nicht erwünscht, dass Karten für zwei verschiedene Systeme, z.B. Telephonkarten für zwei Länder, austauschbar sind. Für jeden wichtigeren Kartenbenützer wird daher ein eindeutiger Echtheitsschlüssel benötigt. Hier bieten die Geometrie des Lesekanals und die Anzahl der in einem bestimmten Kanal verwendeten Quellen und Detektoren die nötigen Freiheitsgrade, so dass eine hinreichende Anzahl unabhängiger Schlüssel zur Verfügung gestellt werden kann.

Die hier beschriebenen Prinzipien liessen sich nur begrenzt anwenden (das gilt vor allem für Geldersatzkarten), sofern nicht Produktionsverfahren existierten, mit denen grosse Kartenmengen zu einem wirtschaftlichen Preis hergestellt werden können. Ein solches Verfahren steht nunmehr zur Verfügung. Gezielte Entwicklungsarbeiten bei Landis & Gyr während der letzten fünf Jahre haben die Realisierung dieser Technologie ermöglicht (siehe Abschnitt 5).

Bild 3 Kartenkomponenten:
optisch verschlüsselter Kartenteil
neutrale Deckkarte
laminierte und photogravierte Karte

4. Verschlüsselungsstrategie und Sicherheit

4.1 PHONOCARD und verwandte Systeme

Die Herstellung von Geldersatzkarten ist in gewisser Hinsicht mit derjenigen von Banknoten zu vergleichen: Es müssen grosse Mengen von Karten hergestellt werden, die bis auf eine zu Verwaltungszwecken angebrachten laufenden Nummer identisch sind. Die verschiedenen Systeme werden durch jeweils andere optische Echtheitsschlüssel unterschieden. Innerhalb eines einzelnen Geldersatzsystems ist eine weitere Unterteilung der Kartenschlüssel möglich, indem auf jeder Karte ein optischer Vorschlüssel oder eine Adresse gespeichert wird. Dieser Vorschlüssel erlaubt dem Systemanwender weitere Information (z.B. Tarife, Ausgabedatum oder Gültigkeitsdauer der Karte) einzubauen oder ein spezifisches Teilsystem, für das die Karte gelten soll, zuzuweisen. Der Vorschlüssel wird bei der Kartenherstellung angebracht, d.h. die Karten haben unmittelbar nach der Herstellung Geldwert. Daher sind angemessene Sicherheitsmassnahmen bei der Bearbeitung und Endkontrolle der Karten wesentlicher Bestandteil aller Herstellungs- und Verteilungsschritte. Bei den im Umlauf befindlichen Karten ist die Sicherheit gegen betrügerischen Missbrauch des Systems, z.B. Ganz- oder Teilfälschung, durch die komplizierte Verschlüsselung und Herstellungstechnik der Karten gewährleistet. Unter diesem Gesichtspunkt bieten, wie wir glauben, diese Systeme für diese Art von Anwendungen die höchste derzeit existierende Sicherheit.

4.2 System ID 2000

Weil Zutritts- oder Identifizierungskarten personengebunden sind, musste eine Strategie entwickelt werden, welche die Sicherheit der Kartenverschlüsselung bei allen Herstellungs- und Verteilungsschritten gewährleistet ist. Die Karten für das System ID 2000 bestehen aus zwei anfänglich getrennten Bestandteilen, nämlich einer maschinell lesbaren Komponente und einer Komponente mit graphischer Information. Wie bei den Geldersatzsystemen wird der maschinell lesbare Kartenteil mit einem holographischen Schlüssel versehen, der eindeutig einem umfassenden System oder einer Gruppe von Systemen zugeordnet ist. Die soweit hergestellten Karten können noch nicht von einem Zutrittskontroll-Lesegerät gelesen werden, sondern müssen zuerst noch zwei weitere Verschlüsselungsschritte in zwei getrennten Kartenprogrammiereinheiten durchlaufen. Der erste Schritt besteht in einer verschlüsselten Folge von Löschoperationen optischer Muster und dient der Zuweisung eines bestimmten Teilsystems. Dieser erste Schritt wird vom Kartenhersteller ausgeführt. Der zweite Schritt dient der Verschlüsselung individueller Benützerinformation. Bei Anwendungen mit hohen Sicherheitsansprüchen wird die zweite Programmiereinheit vom Systemanwender betrieben. Dieser kann dann einen Algorithmus bestimmen, der die zur verschlüsselnde, personenbezogene Information in eine bestimmte, auf der Karte zu speichernde Schlüsselfolge umsetzt. Die Programmiereinheit des Anwenders akzeptiert nur Karten, welche die richtige Teilsystem-Adresse enthalten.

So bleiben die Schlüsselfolge und die individuelle Benützerinformation dem Personal des Kartenherstellers unbekannt. Darüber hinaus kann der Systemanwender nur solche Karten programmieren, die für sein eigenes System bestimmt sind. Nach Verschlüsselung der richtigen Information wird der codierte Kartenteil mit der zweiten Komponente, welche die graphische Information trägt, verschweisst. Das geschieht mittels einer eigens entwickelten Laminiervorrichtung. Der graphische Kartenteil ist entweder neutral, d.h. er enthält keinerlei personenbezogene Information, oder er ist personenbezogen und enthält eine eingravierte Photographie des Karteninhabers und weitere personenbezogene Information wie z.B. eine Unterschrift und eine Abteilungsnummer. Je nach Wahl des zweiten Kartenteils kann die fertige Gesamtkarte entweder als einfache Zutrittskontrollkarte oder als kombinierte Identifizierungs- und Zutrittskontrollkarte benutzt werden. Bedeutende Systemanwender können daher selbst beide Kartentypen ver-

schlüsseln und ausgeben. Daraus ergibt sich ein Höchstmass an Sicherheit und eine möglichst geringe Wartezeit bei der Ausgabe von neuen oder der Ersetzung von alten Karten. *Bild 3* und *4* zeigen Beispiele für die verschiedenen Kartenteile sowie die drei Geräte – Programmiereinheit, Photograviereinheit und Laminiereinheit – die bei der Herstellung des personenbezogenen Kartenteils benutzt werden.

5. Technologie der Kartenherstellung

5.1 Druckmatrizen

Grundlage der Massenproduktion von Karten für die hier beschriebenen Anwendungen ist die Herstellung spezieller Druckmatrizen, die zur Erzeugung der optischen Information mit hoher räumlicher Auflösung in der Kartenstruktur dienen.

Die Druckmatrizen sind das Ergebnis einer Reihe von sorgfältig überwachten Herstellungsschritten, deren erster die holographische Aufzeichnung des Echtheitsmusters für ein bestimmtes System in einem geeigneten lichtempfindlichen Material ist. Die kohärente Strahlung für diese Aufzeichnung liefert ein Laser. Die holographische Aufzeichnung wird unter Bedingungen höchster mechanischer und thermischer Stabilität vorgenommen. Das dazu dienende optische System ist vollständig von Schwingungen des Gebäudes und Temperaturschwankungen zu isolieren. Die belichtete Aufnahme wird entwickelt. Dann werden eine Reihe von Metallkopien der Aufzeichnung gemacht, und diese werden zu Druckplatten für die Kartenherstellung verarbeitet. Jede Druckplatte kann wiederholt zur Herstellung grosser Kartenmengen verwendet werden.

5.2 Kartenherstellung

Die Kartenherstellung beginnt mit der Bearbeitung eines geeigneten Substratmaterials. Das Material kommt von zwei Plastikfolien, die am Anfang der Produktionslinie miteinander verschweisst werden (Laminierung). Jede Folie hat strenge Anforderungen im Hinblick auf Homogenität und optische Eigenschaften zu erfüllen und wird unter Bedingungen grösster Sauberkeit weiter verarbeitet. Nach der Laminierung werden Leerkarten aus der Folie gestanzt und durch einen chemischen Reinigungsprozess für den Druckvorgang vorbereitet. Dann wird die optische Information, die eine Werteinheit oder ein Identifizierungsfeld darstellt, von der Druckmatrize auf die Leerkarte übertragen. Nach dem Druck wird die optische Information mit einem Schutzlack überdeckt, der u.a. auch dazu dient, die Information während der Lebensdauer der Karte vor Beschädigung zu schützen. Nach Funktionsprüfung und Endkontrolle werden die Karten mit einer laufenden Nummer versehen und versandbereit verpackt.

Die Vorgänge bei der Kartenherstellung erlauben, abgesehen von der visuellen Qualitätskontrolle auf Schönheitsfehler, einen hohen Automatisierungsgrad. Diese Automatisierung wird gegenwärtig im Produktionsbetrieb eingeführt. Die Automatisierung wirkt nicht nur kostensenkend, sondern spielt auch bei der Aufrechterhaltung höchster Sauberkeit eine wesentliche Rolle, weil so die Karten fast nicht von Menschenhand berührt werden.

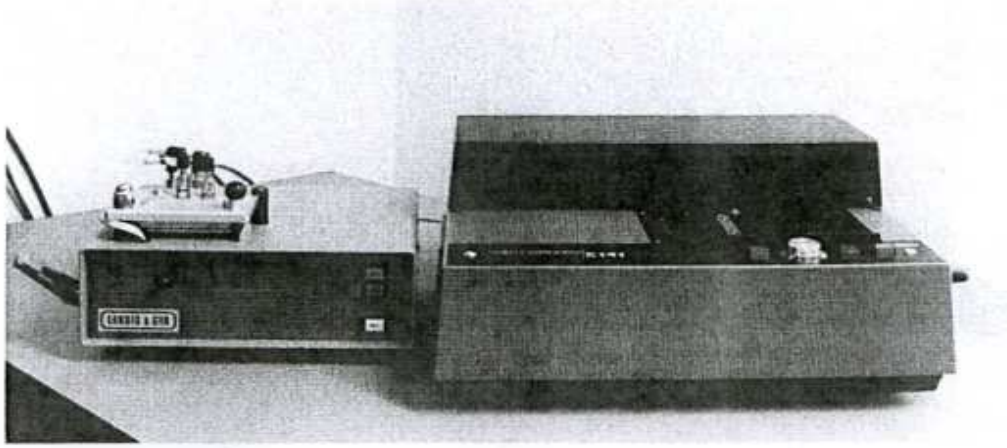
5.3 Qualitätsprüfung und Sicherheitskontrolle

Hier sind verschiedene Aspekte zu erwähnen. Zunächst müssen alle Karten eine Reihe optischer Kriterien erfüllen, die sicherstellen, dass die Karten später von den Lesegeräten akzeptiert werden. Bei Geldersatzkarten, bei denen jede Einheit einen Geldwert darstellt, heisst das, dass die optischen Eigenschaften einer jeden Einheit geprüft werden müssen. Im Falle einer Geldersatzkarte mit 120 Einheiten werden für jede Karte einige hundert Messungen benötigt. Dabei muss jedes gemessene Signal zwischen vorgegebenen absoluten Minimal- und Maximalwerten liegen. Diese Messungen werden mittels einer automatischen Prüfeinrichtung vorgenommen, wobei Karten einem Vorratsbehälter entnommen werden und durch eine Hochgeschwindigkeitsmessvorrichtung geschickt werden. Mangelhafte Karten werden automatisch aussortiert. Ein Tischrechner wertet die Messignale aus und ermittelt ebenfalls die Messstatistik für jede Kartenserie. Ausgeschiedene Karten werden vernichtet und dürfen die Produktionsstätte nicht verlassen, es sei denn, sie werden zur weiteren Auswertung benötigt. Zusätzlich zur optischen Prüfung ist die genaue Kontrolle aller Kartenabmessungen notwendig, damit sichergestellt ist, dass die Karten richtig in das Lesegerät eingeführt werden können. Ferner wird die Kartenqualität visuell geprüft, um Karten auszuscheiden, die z.B. fehlerhaften Druck oder andere Oberflächenfehler aufweisen.

Ähnlich wie bei der Herstellung von Banknoten oder anderen Sicherheitsdokumenten besteht auch bei der Kartenproduktion das wichtige Problem der Sicherheitskontrolle bei allen Produktionsvorgängen. Eine solche Kontrolle erfolgt auf drei Ebenen:

1. Begrenzung des Zugangs zu der beträchtlichen Menge technischer Information und den Einzelheiten der Verschlüsselung, die bei der ganzen Produktionskette eine Rolle spielen.
2. Physische Sicherheitsmassnahmen zum Schutz empfindlicher Materialien (z.B. Druckmatrizen und Vorräte fertiger Karten) in der Produktionsstätte und
3. Lager- und Buchhaltungssystem, das die vollständige Kontrolle über alle hergestellten Karten ermöglicht.

Bild 4 Zum Anbringen personenbezogener Karteninformation benötigte Ausrüstung: Programmiereinheit



Laminiereinheit und Photograviereinheit

Diese Sicherheitsmassnahmen führen zu unvermeidbaren erhöhten Kosten der Kartenproduktion. Der Zugang zu allen Räumen, in denen z.B. Matrizen und Karten hergestellt werden, ist beschränkt und durch ein Zutrittskontrollsystem geschützt. Besucher sind stets durch berechtigtes Personal zu begleiten. Alarmsysteme melden unberechtigtes Eindringen ausserhalb der Arbeitszeit.

6. Kartenleser und verwandte Geräte

6.1 PHONOCARD und ähnliche Systeme

Die PHONOCARD-Station besteht aus zwei Grundeinheiten: dem Kartenleser mit seiner Elektronik und der zum Telephonsystem gehörenden Elektronik, die mit dem Kartenleser und auch mit der Telephonlinie, dem Hörer und dem Wählmechanismus verbunden ist. Hier betrachten wir nur die Leseeinheit. Die Karten werden gegen einen leichten Federdruck durch einen Schlitz in der Frontplatte des Gehäuses eingeführt. Eine halbkreisförmige Aussparung in der Mitte des Schlitzes erlaubt, dass ein Teil der eingeführten Karte sichtbar bleibt. So vergisst man weniger, die Karte nach dem Gespräch wieder herauszunehmen. Der Kartenleser enthält einen Klemm-Mechanismus, der dafür sorgt, dass die Karte nicht während eines Gesprächs herausgezogen werden kann. Der Klemm-Mechanismus wird nicht betätigt, wenn eine ungültige Karte (z.B. eine leere oder eine zu einem anderen System gehörenden Karte) eingeführt wird oder wenn die Stromversorgung ausgefallen ist. In diesen Fällen wird die Karte sofort ein Stück weit aus dem Schlitz zurückgeschoben. Die Karte wird ebenfalls ausgeworfen, wenn alle Werteinheiten verbraucht sind oder wenn das Gespräch durch Auflegen des Hörers beendet ist. Die auf einer gültigen Karte verbliebenen Werteinheiten können jederzeit geprüft werden, indem man die Karte einführt ohne den Hörer abzunehmen. Eine Flüssigkristall-Anzeige zeigt die Anzahl der verbliebenen Einheiten an, und nach einer Sekunde wird die Karte wieder ausgeworfen. Bei einem normalen Gespräch wird zunächst der Hörer abgenommen und die Karte eingeführt. Ein kleiner Schrittmotor treibt einen optischen Lesekopf an, der zunächst den Echtheitsschlüssel abtastet, um die Gültigkeit der Karte zu prüfen, und dann die einzelnen Werteinheiten, um sowohl die Echtheit als auch den verbliebenen Wert festzustellen. Dann wird die Nummer gewählt (Tastenwähler). Wenn die Verbindung hergestellt ist, überträgt ein Löschkopf einen kurzen Wärmestoss auf das Feld einer Werteinheit durch Kontakt mit der Karte. Während des Löschvorgangs wird die Änderung des optischen Signals verfolgt; sobald die erwartete Änderung gemessen ist, fahren Lese- und Löschkopf zum nächsten Wertfeld und die Echtheitsprüfung wird wiederholt. Die zeitliche Abfolge der Löschvorgänge wird natürlich durch die Entfernung zwischen den Gesprächsteilnehmern bestimmt, und die dazu nötigen Zeitimpulse werden durch die Linie von der Zentrale übermittelt. Der PHONOCARD-Leser kann bis zu drei Gesprächseinheiten pro Sekunde löschen und kann daher, falls gewünscht, sogar für Überseegespräche benutzt werden. Es ist ferner möglich, dass der Anrufer während des Gesprächs eine verbrauchte Karte durch eine neue ersetzen kann, ohne das Gespräch unterbrechen zu müssen. 15 Sekunden bevor eine Karte abgelaufen ist, wird dies dem Benützer durch ein Blinklicht gemeldet. Dann kann dieser eine Taste drücken, die bewirkt, dass die restlichen Werteinheiten elektronisch gespeichert und auf der Karte gelöscht werden. Dies ermöglicht das Einführen einer neuen Karte ohne Unterbrechen der Verbindung.

Für die Anwendung von Geldersatzkarten ausserhalb der Fernsprechbranche, und wo eine hohe Wertkapazität und schnelle Entwertung benötigt werden, wurde zusammen mit der Firma Zühlke Engineering AG (Schlieren) ein Kartenleser anderer Art entwickelt. Dieser Kartenleser ist mit einem Transportmechanismus ausgerüstet, der die eingeführte Karte ganz in den Leser hineinzieht und erlaubt auch die Einführung einer zweiten Karte als Reserve. Die Karten für dieses System haben ein grösseres Wertfeld und sind mit 200 Werteinheiten (neben dem Adressfeld) versehen. Der Entwertungsvorgang erfolgt mit einer Frequenz von ca. 10 Werteinheiten pro Sekunde. Kartenleser beim Einkassieren von Parkgebühren in der Zürcher Innenstadt sind seit Frühjahr 1980 in Betrieb.

6.2 Das System ID 2000

Der Zutrittskontrolleser ID 2000 enthält keinen motorgetriebenen Transportmechanismus; vielmehr wird die Karte gelesen, während sie von Hand durch den vertikalen Schlitz in der Frontplatte geschoben wird (siehe *Bild 2*). Das braucht nicht mit konstanter Geschwindigkeit zu geschehen. Während des ganzen Lesevorgangs hält der Benützer die Kante der Karte in der Hand. Das hat den Vorteil, dass die Karte nicht im Lesegerät vergessen werden kann. Der Kartenleser ist mit oder ohne Tastatur erhältlich und daher nicht nur für Anwendungen mit Datenspeicherung (Zeitkontrolle usw. brauchbar, sondern auch für die Zutrittskontrolle mit hohen Sicherheitsanforderungen, bei der eine geheime persönliche Nummer eingegeben werden muss. Werden die Lesegeräte als autonome Einheit verwendet, benötigen sie nur eine Niederspannungs-Stromversorgung. Die eingebaute Logik stellt die Gültigkeit oder Ungültigkeit einer eingeführten Karte fest (wobei auch mit einer beschränkten „schwarzen Liste" verglichen wird, um unerwünschte Karten auszuschliessen) und liefert Signale an eine Reihe von spannungsfreien Kontakten. Diese Kontakte dienen zur direkten Ansteuerung einer Spule (die eine Tür öffnet), einer Vorrichtung zur Überbrückung einer Sperre (für das Verlassen einer Zone mit beschränkter Zugangsberechtigung) und optischer oder akustischer Alarmvorrichtungen, die Betriebsstörungen melden.

Die Kartenleser können an eine zentrale Datenverarbeitungseinheit angeschlossen werden. Das erlaubt den Einbau einer Reihe von zusätzlichen Funktionen. Dazu gehören lückenlose Datenaufzeichnung zu Sicherheits-und Zeiterfassungszwecken, unmittelbare Bildschirmdarstellung des gesamten Personenverkehrs im System, die Aufrechterhaltung einer umfassenderen „schwarzen Liste" unerwünschter oder blockierter Karten und die sofortige zentrale Meldung von Störungen über eine Reihe von Alarmsignalen. Neben dem Kartenleser und der zentralen Datenverarbeitungseinheit wird für den vollen Einsatz des Systems ID 2000 noch zusätzlich die in *Bild 4* gezeigte Ausrüstung benötigt. Bei höchsten Sicherheitsansprüchen oder Grossanwendern können diese Einheiten an Ort und Stelle aufgestellt und vom Büropersonal bedient werden. Die beiden Versionen der Programmiereinheit (Verschlüsselung der Anwenderadresse und Verschlüsselung der personenbezogenen Information) sind mechanisch ähnlich, unterscheiden sich aber in der internen logischen Anordnung, damit die beiden Verschlüsselungsvorgänge getrennt bleiben. Die nötige Karteninformation wird mittels einer Tastatur eingegeben, und die Schlüsselsequenzen werden automatisch auf eine eingeführte Karte übertragen.

Falls photographische Identifizierung notwendig ist, wird der zweite Kartenteil mit Feldern versehen, in die ein Photo und andere personenbezogene Informationen eingraviert werden können. Die Photogravierung wird durch eine im Handel erhältliche Einheit ausgeführt, die ein gewöhnliches Passphoto in ein auf der Karte eingraviertes schwarzweiss Halbtonbild umsetzt.

Falls man kein Photo des Karteninhabers benötigt, wird eine neutrale zweite Kartenkomponente geliefert, die mit geeigneter Graphik bedruckt ist.

Die beiden Komponenten, aus denen nachher die fertige Karte besteht, werden mittels einer kleinen, eigens zu diesem Zweck entworfenen Laminiereinheit zusammengefügt. Es werden keinerlei zusätzliche Klebstoffe benötigt. Die beiden Kartenteile werden in eine Schablone eingeführt und durch einen automatischen Heiz- und Kühlzyklus miteinander verschweisst. Nach der Laminierung können die beiden Komponenten nicht mehr voneinander getrennt werden, ohne dass die Karte zerstört wird.

7. Das Verhältnis von Sicherheit und Kosten

Wie der obigen Beschreibung zu entnehmen ist, liegen Geldersatz- und Identifizierungssystemen verschiedenartige Sicherheitserwägungen zugrunde. Im allgemeinen bedeutet höhere Sicherheit auch höhere Kosten für den Anwender. Von den Kosten her gesehen, liegen die hier beschriebenen Systeme ungefähr im mittleren Bereich dessen, was das Spektrum der heutigen Technologie bietet: Systeme mit Verschlüsselung durch gestanzte Löcher oder einfache Magnetstreifen sind zweifellos billiger, sowohl was das Lesegerät als auch was den Informationsträger anbetrifft, aber sie bieten nur geringe Sicherheit. Systeme, die beispielsweise mit automatischer Erkennung eines Stimm-Abdrucks, eines Fingerabdrucks oder einer Unterschrift arbeiten, haben zwar ein sehr hohes Sicherheitspotential, sind aber sehr teuer und dürften zudem für einige Anwendungen ungeeignet oder ästhetisch unzumutbar sein.

Bei einer bestimmten Anwendung ist das Sicherheitsbedürfnis am gesamten in Frage stehenden Wert zu messen. Bei einem System mit einer grossen Anzahl von Transaktionen mit kleinem Einzelwert (wie z.B. PHONOCARD) ist dieser Gesamtwert durch die Summe des Werts aller gleichzeitig in Umlauf befindlichen Karten gegeben. An ein solches System dürften etwa die gleichen Sicherheitsansprüche gestellt werden wie an ein System mit einer sehr beschränkten Anzahl Transaktionen mit grossem Risiko (der nur Berechtigten vorbehaltene Zugang z.B. von Bankangestellten zu einer Bank).

Beim System PHONOCARD darf die Sicherheit nicht auf dem Lesegerät beruhen, denn der Diebstahl einer Fernsprechstation wäre für einen Verbrecher kein Problem. Sie muss vielmehr in der Kartentechnologie und natürlich auch in der Organisation, welche die Karten herstellt und verteilt, begründet sein. Dieses Konzept erlaubt eine kostengünstige Herstellung der Kartenleser, was in jedem Fall eine wesentliche Forderung ist. Die Kosten der komplexen Technologie, die zur Herstellung der Karten notwendig ist, sind angesichts der grossen Anzahl von Karten, die das System erfordert, vertretbar.

Beim Zutrittskontrollsystem ID 2000 ist die Sicherheit verteilt auf die Karte, die logistische Kette, welche die Verschlüsselung der Karte im Endzustand überwacht, und das Lesegerät zusammen mit irgendeinem Datenverarbeitungsgerät, das imstande ist, die Karteninformation zu interpretieren. Der gesamte Preis für die Sicherheit ist notwendigerweise höher als beim PHONOCARD-System, denn es wird eine umfassendere Reihe von Geräten benötigt, die Stückzahlen sind kleiner, und es sind wegen der personenbezogenen Information auf der Karte mehrere getrennte Herstellungsschritte nötig. Ausserdem ist bei der Installierung eines sicheren Zutrittskontrollsystems auch die physische („Ziegelsteine und Mörtel") Sicherheit des geschützten Bereichs zu beachten. Ferner ist sicherzustellen, dass das System in verantwortungsvoller Weise benutzt wird.

Abschliessend ist zu bemerken, dass Sicherheit immer relativ ist: Es gibt kein System, das absolut sicher gegen verbrecherischen Missbrauch ist. Im Falle der beiden hier beschriebenen Systeme wurde die der Technologie innewohnende Sicherheit den speziellen Anforderungen an das System angepasst. Wir glauben, dass der finanzielle Aufwand und das technische Wissen, deren es für einen ernsthaften Betrugsversuch bedarf, eine mehr als hinreichende Abschreckung darstellt.

8. Dank

Das System PHONOCARD, das dazugehörige Geldersatzsystem und das Zutrittskontrollsystem ID 2000 wurden dank der gemeinsamen Aktivität verschiedener Bereiche des Landis & Gyr-Konzerns verwirklicht. Es ist nicht möglich, hier alle Mitarbeiter, die bei den vielfältigen Arbeiten mitgewirkt haben, namentlich aufzuführen. Dank und Anerkennung für Einsatz, gute Zusammenarbeit und Unterstützung gebühren dem Personal des Zentralen Forschungs- und Entwicklungslabors von Landis & Gyr in Zug, des Produktebereichs Telephonie von Sodeco-Saia in Genf, des Produktebereichs Comfort-Control Systeme von Landis & Gyr in Zug und der Fabrikationsbereiche von Landis & Gyr in Zug, die an der Realisierung der beschriebenen Systeme beteiligt waren.

Autor: David L. Greenaway
LGZ Landis & Gyr Zug AG
CH-6301 Zug (Schweiz)

Übersetzer: H. und G. Baltes
LGZ Landis & Gyr Zug AG