

ASA NEWS

Die Rolle kontaktloser Chipkarten im Banking

Jüngste Trends im Bereich kontaktloser Chipkarten und technische Entwicklungen, wie MIFARE® PLUS, die kontakt und kontaktlose Schnittstellen auf einem Chip vereinen, erlauben erweiterte Anwendungsmöglichkeiten von Bankkarten.



Könnten Sie sich einen Fernseher ohne Fernbedienung noch vorstellen? Was haben Zentralverriegelung, Fernbedienung, Funkschlüssel und kontaktlose Chipkarten gemeinsam?

Es sind technische Lösungen, die dem Benutzer mehr Komfort bieten. Nachdem man sich an Annehmlichkeiten gewöhnt hat, will man diese nicht mehr missen. Wie die Vergangenheit gezeigt hat, trägt Komfort also stark zur Entwicklung und zum Einsatz von technischen Innovationen bei.

Beispielsweise Chipkarten, und hier im besonderen Chipkarten mit kontaktloser Schnittstelle, können das Leben wesentlich vereinfachen, da man auch ohne Klein- und Wechselgeld das Auslangen findet. Dazu ein Vergleich: Für eine Transaktion mit einer Kontaktchipkarte sind folgende Schritte nötig:

Geldbörse herausnehmen; öffnen; die Karte heraussuchen (üblicherweise hat man schon einige Karten in der Geldbörse, wobei die Tendenz steigend ist); herausziehen; in die richtige Position

Nr. 5 Dezember 1996

Inhalt

<i>Die Rolle kontaktloser Chipkarten im Banking</i>	1
<i>Verwendung in Seoul</i>	3
<i>Trend zur Chipkarte</i>	3
<i>Der Weg zur kontaktlosen Karte</i>	4
<i>Technische Lösungen</i>	4
<i>Zusammenfassung</i>	5
CASSAMAT	6
<i>Elektronische Geldbörse bei Raiffeisen Südtirol</i>	6
Kryptographie und Politik	7
<i>Soll die Verschlüsselung gesetzlich beschränkt werden ?</i>	7
Veranstaltungen	10
<i>Konferenzen, Messen</i>	10
GENERAL-VERSAMMLUNG	12

Impressum: Informationsschrift für die Mitglieder der ASA,

Herausgeber:

Austrian Smart Card Association - Österreichische Chipkarten Vereinigung,

A 1127 Wien, Postfach 81, Tel.: (0222) 61 51 134-751, FAX: (0222) 61 51 134-777

email: asa@ict.tuwien.ac.at, DVR: 0698121

bringen (ist speziell für ältere Personen kein leichtes Unterfangen) und in den Schlitz stecken, vorausgesetzt daß dieser nicht mit Kaugummi verklebt ist; warten, was im Gedränge oft nicht sehr angenehm ist; hat man die Karte richtig hineingesteckt, diese wieder herausnehmen und zurück in die Geldbörse geben.

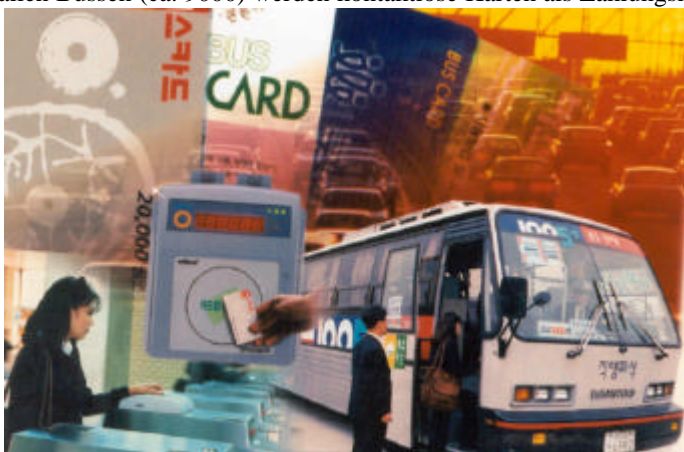
Mit einer berührungslosen Proximity-Karte mit einer Arbeitsentfernung von bis zu 10 cm sieht eine Transaktion wesentlich einfacher aus:

Geldbörse herausnehmen, an der Oberfläche des Terminals vorbeiführen, nach Beenden der Transaktion ertönt ein Signal (die Transaktionszeit beträgt bei schnellen Systemen weniger als 1/10 Sekunden), fertig.

Haben Kartenbenützer die Wahlmöglichkeit zwischen den beiden Systemen, so wird ein hoher Prozentsatz die bequemere Variante vorziehen. Die Reichweite des kontaktlosen MIFARE® Systems ist auf 10 cm beschränkt, da auf diese Weise mit der Transaktion eine bewußte Handlung verbunden ist. Zur Verstärkung dieser bewußten Handlung kann die Terminaloberfläche mit einem leicht bedienbarem Knopf ausgestattet sein, der beim Vorbeiführen der Karte gedrückt wird, um eine Transaktion tatsächlich erfolgen zu lassen.

Verwendung in Seoul

Das Projekt mit den meisten elektronischen Wertkarten-Transaktionen weltweit ist in der 12-Millionen Metropole Seoul. Bis Ende November wurden hier insgesamt 144.000.000 Transaktionen gezählt. In allen Bussen (ca. 9000) werden kontaktlose Karten als Zahlungsmittel akzeptiert, die an ca. 2000 Aufladestationen



wieder aufgeladen werden können. 2,5 Millionen MIFARE® Karten mit täglich ca. 1,7 Millionen Transaktionen zeigen die breite Akzeptanz für die kontaktlose Technologie, die im wesentlichen auf der einfachen Handhabung der Karte beruht.

Das erfolgreiche "Bus Card"-System wird derzeit auch auf die umliegende Provinz Kyung Ki und die Insel Cheju ausgeweitet. Somit werden Ende 1996 in ganz Korea 13.000 Busse mit kontaktlosen Terminals ausgerüstet und 3.500 Aufladestationen installiert sein. Der mit der Installation betraute koreanische Systemintegrator Intec schätzt, daß in den

nächsten 12 Monaten weitere 10 Millionen Karten ausgegeben werden.

Weiters hat die Stadtregierung von Seoul angekündigt ein kompatibles System auch für die U-Bahn einzuführen. Zusätzlich zur Ticketing Anwendung wird die universell einsetzbare kontaktlose "Bus Card" in Zukunft unter anderem auch als elektronische Geldbörse, Kundenkarte und ID Card eingesetzt werden.

Trend zur Chipkarte

Die klaren Vorteile der Chipkarte, wie beispielsweise Effizienzsteigerung, wurden erkannt. Allgemein wird der Einsatz von Bankkarten mit Chip in den nächsten Jahren stark ansteigen. Im europäischen Raum sind dies typischerweise Kontaktchipkarten, wie in Deutschland oder Österreich. Dieses System wird jedoch nur dann erfolgreich sein, wenn es akzeptiert wird und die Karten auch entsprechend oft verwendet werden. Dazu benötigt man Treiberanwendungen, also Anwendungen bei denen die Karten erstens oft benutzt werden und zweitens für den Anwender von Vorteil sind. Letztlich müssen aber die Vorteile der Systemseite auch klar erkennbare Vorteile für den Kunden bringen. In einigen Anwendungen, wo eben eine häufige Nutzung von Karten gegeben wäre, wie z. B. der Einsatz als elektronisches Ticket, verstärkt sich der Wunsch, die Transaktionen auch komfortabel durchführen zu können.

Der Weg zur kontaktlosen Karte

Auf der einen Seite haben wir eine etablierte kontaktbehaftete Infrastruktur, auf der anderen Seite den Wunsch über komfortable Add-on Features dem Kartenbenützer weitere Vorteile zu bieten und damit eine noch stärkere



Nutzung der Karten zu erreichen. Eine Brücke zwischen diesen beiden Welten ist nun eine Karte mit zwei Schnittstellen. Einerseits eine kontaktbehaftete Schnittstelle zur Nutzung der Infrastruktur und Verwendung der Funktionen, die heute bei kontaktbehafteten Systemen implementiert werden, und andererseits eine kontaktlose Schnittstelle. Somit kann auch ein noch breiteres Anwendungsspektrum angeboten werden. Es ist nun möglich mit ein und derselben Karte die elektronische Geldbörse über die Kontaktschnittstelle zu nutzen, aber diese Karte auch als elektronischen Fahrschein, als Stadionticket oder im Tourismusbereich über die bequeme kontaktlose Schnittstelle zu betreiben. Nachdem man sich an die neue Technologie gewöhnt und die Vorteile der kontaktlosen Schnittstelle erkannt hat, wird

auch verstärkt das Interesse steigen berührungslos bezahlen zu wollen.

Mit einer solchen kombinierten Karte können Systembetreiber Lösungen anbieten, die den verschiedenen Bedürfnissen ihrer Kunden entsprechen. Eine Produktpalette, bei der der Kartenbenützer selbst entscheiden kann, welche Art von Transaktionen bzw. Applikationen er auf seiner Karte laufen lassen möchte und über welche Schnittstellen diese abwickelt werden sollen, wird durch eine den Kundenwünschen angepaßte Leistungserbringung den Weg zur breiten Akzeptanz dieser Karten ebnen.

In Asien, wo eine andere Kultur mit niedrigeren Hemmschwellen zu neuen Technologien existiert, wird sich die neue Technologie mit all seinen Vorteilen schon früher durchsetzen, wie sich bereits am Beispiel Seoul gezeigt hat.

Technische Lösungen

Technische Lösungen dazu werden z. B. von Philips/Mikron entwickelt, wo zunächst zwei bestehende Welten verschmolzen werden. Zwei bekannte und erprobte Technologien, ein kontaktbehafteter Mikroprozessor, der mit verschiedenen Betriebssystemen arbeiten kann, und eine berührungslos funktionierende MIFARE®-Schnittstelle mit dazugehöriger Steuerlogik, werden auf einem Chip integriert. Dieser MIFARE® PLUS Chip ermöglicht, die vorhandenen Datenspeicherressourcen in Abhängigkeit der Schnittstellen nach den speziellen Anforderungen der jeweiligen Anwendung zu konfigurieren. Es stehen Speicherbereiche zur Verfügung, die beispielsweise nur über die kontaktbehaftete Schnittstelle zugänglich sind oder solche, wo ein Zugriff nur über die kontaktlose Schnittstelle möglich ist, einen Bereich, wo beide Schnittstellen zugreifen können und einen Bereich, wo von kontaktloser Seite Werte nur abgebucht werden können und ein Nachladen einer elektronischen Börse nur über die Kontaktschnittstelle möglich ist. Durch geeignete Betriebssysteme kann dieser Chip bei bestehenden Anwendungen für Kontaktkarten völlig kompatibel eingesetzt werden, wobei Add-on Funktionen über die kontaktlose MIFARE® Schnittstelle ermöglicht werden.

In einem nächsten Schritt wird die MIFARE® Architekturplattform um leistungsoptimierte, auch berührungslos arbeitende Mikroprozessor Chips erweitert. Hier steuert auch bei kontaktlosen Transaktionen das Betriebssystem die Funktionen des Chips. Letztlich ergibt sich eine Produktfamilie mit verschiedenen Derivaten bis hin zum kontaktlos arbeitenden Kryptocontroller und Abstufungen der Speichergrößen. Hier wird das Know-how von Mikron und Philips ideal in starken Synergien kombiniert. Eine logische Unterscheidung zwischen berührungslosen Chips bzw. Kontaktchips wird es nur mehr im Interfaceteil geben. Über beide Schnittstellen können prinzipiell die gleichen Funktionen mit gleichem Sicherheitsniveau ausgeführt werden. Da der Chipflächenbedarf für ein zusätzliches kontaktbehaftetes Interface bei einem kontaktlosen Mikroprozessor Chip

nur sehr gering ist, können diese Chips entweder als kontaktloser Chip, als kontaktbehafteter Chip oder als Kombinationschip, der beide Schnittstellen unterstützt, betrieben werden.

Auch im Bereich der Fertigungstechnologie für kontaktlose Chipkarten hat es in den letzten zwei Jahren enorme Fortschritte gegeben. Technologien, die den hohen Anforderungen der Banken hinsichtlich Kartenschichtaufbau und Sicherheit entsprechen, wurden entwickelt und lassen sich sowohl bei reinen kontaktlosen als auch bei Kombikarten realisieren.

Zusammenfassung

Technisch sind sowohl kontakt als auch kontaktlose Chipkarten ausgereift. Das sehr positive Echo auf den Einsatz von kontaktlosen Proximity-Karten beweist die Akzeptanz dieser Technologie. Da es immer wichtiger wird mit der Karte auch den entsprechenden Kundennutzen zu bieten, wird der Weg über Komfort zum breiten Einsatz berührungsloser Karten führen. Wenn kontakt und kontaktlose Schnittstellen auf Basis eines Chips gleichzeitig genutzt werden können, wie etwa bei MIFARE® PLUS, können auch Zusatzleistungen und Vorteile zu bestehenden Bankkarten angeboten werden, was wiederum die Gesamtakzeptanz dieser Karten fördert.

Zum Autor:

Dipl.- Ing. Dominik Berger

- 1984 - 92: *Studium der Elektrotechnik an der technischen Hochschule in Graz.*
1991: *Bei der Firma AVL North America Inc. in Detroit tätig.
Planung und Inbetriebnahme von Transputer Motorenprüfständen.*
1992: *Bei der Firma Mikron in Graz maßgeblich an der Entwicklung einer kontaktlosen
Prozessor Smart Card beteiligt.
Seit 1992 aktives Mitglied bei nationalen und internationalen Normierungsgruppen (Önorm
AG17,AG27, ISO/IEC JTC1 SC17 WG8, ISO/IEC JTC1 SC17 WG8/TF1).*
1993: *Assistent der Geschäftsleitung bei Mikron.*
seit 1994: *Produkt Manager für kontaktlose Smart Cards (Produktlinie MIFARE®) ◆*

CASSAMAT

Elektronische Geldbörse bei Raiffeisen Südtirol

Presseaussendung der Raiffeisen Südtirol

Zwei Auslöser waren es, die uns im RIS (Raiffeisen-Informationssystem) veranlaßt haben, das Projekt anzugehen.

Der erste Punkt ist eine strategische Linie der Raiffeisengruppe; nämlich die Zahlungsflüsse weitreichend und automatisch erfassen und auf diese Weise Marktanteile anzuziehen.

Die hohen Beträge des Geschäftslebens im täglichen Transfer laufen über das Raiffeisen-Verbundnetz und darüber hinaus italienweit über ein sehr effizientes Zwischenbanken-Datenetz mit elektronischen Überweisungs- und Inkassosystemen.

Die mittleren Beträge des Geschäftes und des privaten Alltags werden über Schecks abgewickelt. Die „Check Truncation“ im italienischen Netz funktioniert gut, ist aber wie jede Belegautomation eine einseitige und damit unvollständige Maßnahme.

In den letzten Jahren hat in diesem Segment der mittleren Beträge eine echte Automation begonnen sich durchzusetzen.: POS-EFT. Dabei werden Zahlungsvorgänge an der Wurzel des Geschehens erfaßt und vollautomatisch abgewickelt. POS/EFT erfreut sich jährlicher Zuwachsraten von 80%. Diese Online-Zahlungsform ist rationell bei Beträgen über 50 DM.

Darunter gab es bisher nur Kleingeld in bar; mit enormen Kosten für das gesamte Bankensystem einschließlich Zentralbank: Bargeldversorgung, Transport, Bearbeitung und Entsorgung (=Recycling). Eine Baroperation in der Bank verursacht z.B. Kosten um die 10 DM.

Dieses Segment hat etwa den 2,5-fachen Umfang gegenüber dem mittleren; und diesen gewaltigen Strom an täglichem millionenfachen Kleingeldflüssen wollen wir in der Raiffeisengruppe erfassen. Die italienische Zentralbank (Banca d'Italia) unterstützt dieses Projekt sehr wohlwollend, weil auch sie ein vielfaches Interesse daran hat.

Der zweite Punkt ist als Argument noch hautnäher: Die Versorgungsprobleme mit Kleingeld in den Tourismuszentren waren ausschlaggebend 1992/93 in Wolkenstein ein Experiment mit der „Gardena Card“ zu beginnen. Dieser erste Feldtest ist positiv ausgefallen und war Anstoß für die Pilotinstallation „CASSAMAT“ in Meran.

Bei der Wahl der Technologie sind wir als kleinste Gruppe völlig unabhängig von europaweiten parapolitischen Lobbies, wirtschaftlichen Einflußsphären oder bürokratischen Normungsgremien. Deshalb konnten wir uns die letzte, beste und sicherste Technologiestufe wählen: kontaktlose Microprozessor-Chipkarten (AT&T).

Das Ziel ist die Erfassung des örtlichen Zahlungsstromes an Kleingeld. Damit sind wir also nicht wie Kreditkarten von internationaler Kompatibilität abhängig und haben uns ohne Kompromisse für eine innovative Technik (C-less) entscheiden können, um damit den lokalen Markt (domestic) abzudecken.

In diesem Zusammenhang bieten die Raiffeisekassen auch eine „Touristenkarte“ an. Diese zielt hauptsächlich auf die Urlaubsgäste ab, die sich bei Beginn ihres Aufenthaltes am Bankschalter ihre Karte laden lassen, während ihres Aufenthaltes mit der Karte zahlen und eventuelle Restbeträge am Ende des Urlaubes wieder einkassieren.

Dank dieser elektronischen Geldbörse könne sich, so zeigte sich Helmut Stroblmair überzeugt, der Urlauber viel ungezwungener und frei von sämtlichen Sorgen um das Wechselgeld und den Verlust seiner Barschaft bewegen.

Nach der landesweiten Einführung wäre es der Wunsch, das Cassamat-System großräumig auszuweiten und in sämtlichen Banken einzubinden.

Presseaussendung der Raiffeisen Südtirol



Kryptographie und Politik

Manfred Holzbach

Soll die Verschlüsselung gesetzlich beschränkt werden ?

Nehmen wir an, Sie sind ein Wirtschaftstreibender, der - wie von vielen Seiten propagiert - seine Geschäftskorrespondenz, Bankgeschäfte und Informationsbeschaffung weg vom Papier hin zur perfekten Illusion auf seinem PC-Bildschirm bringen möchte. Angebote werden mit Text, Logos und bunten Bildchen versehen, mit der Adreßdatenbank zu einer Aussendung vermischt und über die ganze Welt versandt. Die Bestellungen kommen umgehend via E-Mail herein, werden automatisch mit Rechnungen beantwortet, der automatisierte Warenversand beglückt die Besteller mit Ihren Produkten und via elektronischem Kontoauszug sehen Sie erfreut Ihren Ertrag wachsen. Eingekauft wird ebenfalls elektronisch, für neue Produktideen pflegen Ihre Spezialisten eine intensive Korrespondenz mit Designern, Lieferanten und Finanzberatern. Ihre Zahlungen laufen selbstverständlich auch automatisch zur Hausbank, die Ihnen gleich die Daten für das Cash Management mitliefert.

Wunderbare Welt, könnte man meinen, und das alles gibt es schon ! Allerdings wollen Sie es mit richtigen Geschäftspartnern zu tun haben, die real existieren und diese sollen auch zu den von ihnen eingegangenen Verpflichtungen stehen. Außerdem wollen Sie vermutlich nicht, daß andere Ihren schönen Finanzplan und die Kontoauszüge dazu nutzen, über Ihre Bonität und Zahlungsgewohnheiten Bescheid zu wissen. Schon gar nicht, daß Ihre Konkurrenten das Material für Ihre neuen Produkte abfangen.

Alles was Sie noch brauchen, ist eine elektronische Form der rechtsgültigen Unterschrift und ein elektronischer Briefumschlag. Dies ist das Anwendungsgebiet der Kryptographie, das ist die Wissenschaft von der Ver- und Entschlüsselung. Sie können ihre vertraulichen Geschäftsunterlagen mit einem geheimen Schlüssel, einer zufällig erzeugten Zahlenkombination, so vermischen, daß jeder Lauscher in der Leitung nur Datensalat hört oder sieht. Dem befugten Empfänger haben Sie einen passenden Schlüssel zukommen lassen, mit dessen Hilfe er Ihre Botschaft wieder lesbar machen kann. In Erweiterung dieses Verfahrens können Sie damit dem Empfänger, aber auch Dritten (z.B. einem Gericht) nachweisen, daß die Daten von Ihnen stammen und auf dem Weg nicht verändert wurden - damit gelten sie als von Ihnen unterschrieben, auch wenn diese Digitale Signatur ganz anders aussieht als eine eigenhändige Unterschrift.

Was ist also das Problem ? Es gibt bereits jede Menge Hard- und Software, zum Teil ist sie bereits im Einsatz. Logischerweise soll ein solches Verfahren möglichst einheitlich auf der ganzen Welt anwendbar sein. In praktisch jedem Kulturkreis gibt es verschlossene Briefkuverts und menschliche Unterschriften sind als Ausdruck des Willens anerkannt. In der Technik gibt es jedoch eine Vielfalt an Unterschieden, die dazu führen, daß die Systeme nicht „miteinander können“, auch wenn ihre Besitzer es wollen. Dies ist eine Normierungsaufgabe, die bereits angelaufen ist und hier nicht weiter besprochen werden soll.

Ein neues Problem liegt im rechtlichen Bereich und betrifft die Geheimhaltung von Daten generell: Darf man denn Botschaften verschlüsseln ? Man muß richtigerweise davon ausgehen, daß diese neuen Methoden auch von bösen Menschen verwendet werden: Terroristen könnten den nächsten Anschlag mittels verschlüsselten Botschaften planen und Betrüger könnten auch versuchen, digitale Signaturen für unlautere Zwecke zu nützen.

Betrachten wir die Verschlüsselung genauer: Sie unterscheidet sich von einem Briefumschlag ganz wesentlich: Den Briefumschlag kann man aufreißen, wenn der Inhalt z.B. für die Fahndungsbehörde wichtig genug erscheint, und dann kann sie ihn lesen. Eine ausreichend stark verschlüsselte Botschaft bleibt Datenwirrwarr, was immer auch unternommen wird. Keine angenehme Vision für Polizei, Verfassungsschutz und um die nationale Sicherheit besorgte Geheimdienste, allen voran den amerikanischen. Der Punkt: wenn jedermann starke Verschlüsselungsverfahren anwenden kann, so kann man nicht mehr unterscheiden, ob es sich um „normale“ vertrauliche Geschäftspost oder Botschaften mit verbrecherischem Inhalt handelt. Dem stehen die Grundrechte wie Brief-, Geschäfts- und Bankgeheimnis entgegen, die wohl in allen zivilisierten Ländern anerkannt sind. Mehr oder

weniger abhängig vom politischen Stellenwert der „nationalen Sicherheit“ haben sich in verschiedenen Staaten unterschiedliche Gesetzgebungen entwickelt: Während in Frankreich Verschlüsselung mehr oder weniger verboten ist, kann sie in Österreich jeder einsetzen. Die USA gingen zunächst den Weg, den Export starker Verschlüsselungsmechanismen zu verbieten. Dies hatte Folgen: Zum einen konnten amerikanische Hersteller ihre state-of-the-Art Mechanismen nur innerhalb der USA anbieten. Jenseits der Ozeane wiegten sich die Käufer womöglich in der trügerischen Sicherheit, daß ihre Botschaften verschlüsselt seien. Tatsächlich konnte jeder, der ausreichend Zeit und Geld dazu investierte, den Geheimcode knacken, ohne daß dies bemerkt wurde. Die Hersteller aus anderen Ländern hatten einen als unfair bewerteten Wettbewerbsvorteil. Kein Wunder, daß die US-Hersteller Druck auf ihre Regierung machten und gleich eine Lösung anboten: „Key Escrowing“, das bedeutet vereinfacht, daß geheime Schlüssel dann verwendet werden dürfen, wenn man sie zuvor bei einer vertrauenswürdigen Behörde „für alle Fälle“ hinterlegt hat. Bei Verdacht könnte dann etwa das FBI sich die Schlüssel beschaffen und den vertraulichen Nachrichtenverkehr des beobachteten Subjekts mithören. So besann man sich der Rolle als einzige Großmacht und berief im Rahmen der OECD ein Expertenkomitee ein, das anderen Regierungen eine gleichartige Regelung in ihren Ländern schmackhaft machen soll. Darüber hinaus wurde in dieser Sache ein Sonderbotschafter bestellt, der die Argumente sozusagen von Mensch zu Mensch aufbereitet.

Bei allem Verständnis dafür: Wie gefällt Ihnen die Vorstellung, daß Sie sich nur dann einen Safe kaufen dürfen, wenn Sie beim Finanz- oder einem anderen Amt gleich einen Zweitschlüssel dafür und für das Büro hinterlegen müssen ?

Fragen wir uns aber auch, was es denn den Behörden bringen könnte: Angenommen, jeder der seine Schlüssel nicht abliefern, wird bestraft. Egal ob vorsätzlich oder aus Versehen. Mit Jahren im Gefängnis. Wer wird es dann wagen wollen, vertrauliche elektronische Post zu nutzen ? Wohl nur wenige. Wir bleiben beim guten alten Papier. Also sollte nur eine geringe Geldstrafe drohen, wie beim Falschparken: Angenommen, ich verschlüssele unberechtigt die Details eines großen Bankraubs, wird mich die angedrohte Geldstrafe dann abschrecken ? Ok, man findet ein ausgewogenes Maß, alle sind zufrieden und die Leute verschlüsseln, daß die Leitungen glühen: Wen soll die Behörde dann abhören ? Wer ist verdächtig ? Man kann elektronische Post von überall - selbst von Telefonzellen - absenden, als Absender Decknamen verwenden - Und selbst wenn eine „verdächtige“ Nachricht erkannt würde: Man hat sie abgefangen, den dazu passenden Schlüssel und sieht gespannt, wie sich der Klartext offenbart: Pech gehabt, der Inhalt ist nochmals verschlüsselt, diesmal mit einem wirklich geheimen Schlüssel. Also: Einleitung eines Strafverfahrens, Berufung, u.s.w. - dauert Monate, - nur: ist der verschlüsselte Inhalt dann noch von Bedeutung ? Ausgefuchstere Methoden bedienen sich der „Steganographie“: Dies heißt schlicht und einfach, daß der Klartext etwas ganz anderes bedeutet, als es scheint. „Die Tante Mitzi bringt die Torte um 3 Uhr vorbei“ kann dem Empfänger mitteilen, daß die Rauschgiftlieferung um 15h am Flughafen ankommt. Oder verwendet etwa unbenutzte Bits in elektronischen Images, die der Empfänger interpretieren kann. Kein Gesetz kann dies verhindern.

In der Praxis erscheint der Nutzen für die Behörden somit mehr als zweifelhaft. Das räumen sie auch durchaus ein und sind selbst keineswegs überzeugt, damit die großen Fische fangen zu können. Demgegenüber steht ein beträchtliches Potential an Nachteilen für die ehrlichen Benutzer.

Einmal gerufen, wird man die Geister so schnell nicht wieder los. Das Ganze setzt ein beträchtliches Maß an Vertrauen voraus: Angenommen, Sie hinterlegen Ihre geheimen Schlüssel bei einer amtlich ermächtigten Stelle. Damit vertrauen Sie für alle Zukunft, daß diese immer ehrlich und sicher mit ihnen umgeht, sodaß die Schlüssel niemals abhanden kommen oder für andere Zwecke als dem behördlichen Zugriff ausschließlich zum Zweck, ein Verbrechen zu verhindern oder aufzuklären - aufgrund richterlichen Befehls versteht sich - benützt werden. Für digitale Signaturen darf niemand die Möglichkeit haben, sich die geheimen Schlüssel zu beschaffen - auch keine Behörde - sonst kann er beliebig echte Unterschriften auf gefälschte Dokumente anbringen. Diese Stelle wird daher immer die besten Sicherheitsmaßnahmen ergreifen, nur absolut vertrauenswürdige und nicht erpreßbare Mitarbeiter beschäftigen. Das dies alles regelnde Gesetz wird sich niemals zu Ihrem Nachteil ändern, nicht einmal unter extremen Umständen. Selbstverständlich können Sie sich jederzeit überzeugen, daß dies alles ordnungsgemäß abläuft, und wenn allen Maßnahmen zum Trotz dann doch ein Schaden entstehen sollte, wird Behörde jede Haftung übernehmen. Haben Sie dieses Vertrauen ?

Böse Menschen könnten auf die Idee kommen, den dort angesammelten Fundus an geheimen Schlüsseln zu stehlen. Vielleicht sogar unbemerkt, denn alles Gespeicherte läßt sich kopieren. Werden die Verantwortlichen dann auch sofort die Öffentlichkeit über eine solche Panne informieren wollen ? Es muß nicht einmal tatsächlich etwas

passieren, wie steht es mit Ihrem Vertrauen, wenn in Balkenlettern bloß der Verdacht geäußert wird, daß solche Schlüsseldatenbanken etwa für politische Abhöraktionen mißbraucht worden sein sollen ?

Wenn Sie das alles nicht überzeugen sollte, dann reden wir über die Kosten. Sie müssen, um vertrauliche Nachrichten senden und empfangen zu können, eine Behörde kontaktieren. Ein Formular ausfüllen, die Fristen einhalten, eine Bewilligung abwarten, Vorschriften beachten, Gebühren bezahlen. Was bekommen Sie unmittelbar dafür - ganz einfach: nichts. (es sei denn, Sie verkaufen Produkte, welche diese Verfahren unterstützen).

Was hat dies alles mit Smart Cards zu tun ? Nun, diese sind zur Zeit die optimalen Träger für geheime Schlüssel und damit verbundene Operationen, welche sie verwenden. Sie setzen jedem Versuch, darin gespeicherte Informationen unbefugt auszulesen, erheblichen Widerstand entgegen, jedenfalls größeren als andere vergleichbare Medien. Zudem sind sie klein, daher lassen sie sich einfach versenden, herumtragen und wegsperren. Damit und aufgrund des Bedarfs nach elektronischer Vertraulichkeit wird ihnen eine große Zukunft vorhergesagt. Dies wäre mit einem Schlag anders, wenn sich dieser Bedarf verflüchtigen sollte, weil man einen Hauptanwendungsbereich mangels Vertrauenswürdigkeit in Frage stellt. Viele sinnvolle Anwendungen würden wohl von den Benutzern nur kaum akzeptiert: Electronic Banking, Electronic Commerce sowie die zeitgewinnende Nutzung des Internet für den Austausch von wichtigen Geschäftsunterlagen zum Beispiel. Noch viel weniger, wenn es um gespeicherte persönliche Daten oder Geldwerte geht, wie beim elektronischen Krankenschein.

Kein erstrebenswertes Szenario für die Hersteller und Betreiber von Chipkartenanwendungen; und die Dimensionen sind durchaus europäisch: Hier steht nicht weniger als die Zukunft einer Technologie auf dem Spiel, in der gerade Europa die Nase weit vorne hat.

Betrachten wir den zweifelhaften Nutzen von staatlichen Kryptographiebeschränkungen und die damit entstehenden Risiken, dann können wir uns wohl kaum damit anfreunden. Allerdings existiert in diesem Bereich noch wenig an hörbarem Bewußtsein. Bis jetzt haben erst die Banken offiziell ihre Position bezogen. Sie wollen weder, daß ihr Bemühen um Automatisierung des Geldverkehrs zunichte gemacht wird noch womöglich in die Rolle heimlicher Handlanger der Behörden gedrängt werden. Um unlauteren Kunden das Handwerk zu legen, konnte man bisher schon auf richterlichen Befehl die Konten öffnen und die Informationen im Klartext lesen. Daher fordern die Banken von den Regierungsvertretern, sich international keinesfalls zu einer Gesetzgebung zu verpflichten, in denen die Wirksamkeit der Kryptographie untergraben würde. Also keine Beschränkung auf solche Produkte, die mächtige ausländischen Geheimdiensten genehm sind und keine zwangsweise Offenlegung von geheimen Schlüsseln. Andere Wirtschaftssparten sind eingeladen, um nicht zu sagen, aufgefordert, ebenfalls bald eine deutliche Position auszudrücken.

Zum Autor:

Manfred Holzbach,

Projektleiter für Elektronische Unterschrift und Sicherheit von Zahlungssystemen mit Smart Cards in der STUZZA Ges.m.b.H.



Veranstaltungen

Konferenzen, Messen

JANUAR 1997

KW	Mo	Di	Mi	Do	Fr	Sa	So
1			1	2	3	4	5
2	6	7	8	9	10	11	12
3	13	14	15	16	17	18	19
4	20	21	22	23	24	25	26

5	27	28	29	30	31		
---	----	----	----	----	----	--	--

Datum	Thema	Veranstalter	Ort
15.-17.	Omnocard '97, Estrel Hotel	In Time Berlin +49 30 89092 582	Berlin
21.-22.	Purchasing Cards, Arabella Hotel	Management Circle +49 6196 4722 10	Frankfurt
22.-23.	BANKtrendTAGE'97	Management Circle +49 6196 4722 10	Frankfurt
27.-29.	7.6.GMD-SmartCard Workshop	+49 6151 869 206	Darmstadt
30.-31.	Electronic Purse, The Kensington Hilton	SMI	London

FEBRUAR 1997

KW	Mo	Di	Mi	Do	Fr	Sa	So
5						1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28		

Datum	Thema	Veranstalter	Ort
11.-13.	Smart Card '97	QMS Limited +44 733 394304	London

MAI 1997

KW	Mo	Di	Mi	Do	Fr	Sa	So
18				1	2	3	4
19	5	6	7	8	9	10	11
20	12	13	14	15	16	17	18
21	19	20	21	22	23	24	25
22	26	27	28	29	30	31	

Datum	Thema	Veranstalter	Ort
19.-22.	CardTech/SecurTech, Peabody Hotel	CTST, Inc +1 301 881 3383	Orlando
22.-25.	Internet Vision, Messegelände	Leipziger Messe +49 341 678 8288	Leipzig

OKTOBER 1997

KW	Mo	Di	Mi	Do	Fr	Sa	So
40		30	1	2	3	4	5
41	6	7	8	9	10	11	12
42	13	14	15	16	17	18	19
43	20	21	22	23	24	25	26
44	27	28	29	30	31		

Datum **Thema**
30.9.- Eurobank '97, Messe Frankfurt
2.10..

Veranstalter
Info
+31 346 573777

Ort
Frankfurt

*Nach den geruhsamen Weihnachtsfeiertagen
einen guten Beginn im neuen Jahr
sowie viel Erfolg
wünscht Ihnen die
Austrian Smart-Card Association*

Zehnte ordentliche ***GENERALVERSAMMLUNG***

der Austrian Smart-Card Association

Wir gestatten uns, Sie zur neunten, ordentlichen Generalversammlung der Austrian Smart-Card Association einzuladen.

Zeit: Dienstag, 18. Februar 1997, ab 17.00 Uhr
Ort: Technische Universität Wien, Institut für Datenverarbeitung,
Seminarraum, 2. Stock, Gußhausstraße 27-29, 1040 Wien

TAGESORDNUNG

1. Genehmigung der Tagesordnung
2. Festlegung des Protokollführers
3. Rückblick 1996
4. Bericht des Vorstandes für Finanzen
5. Bericht der Rechnungsprüfer und Entlastung des Vorstandes
6. Umbesetzung des Präsidiums
7. Wahl der Rechnungsprüfer
8. Vorschau 1997
9. Anträge
10. Allfälliges

für den Vorstand

gez. Wolfgang Radlwimmer