

ASA NEWS

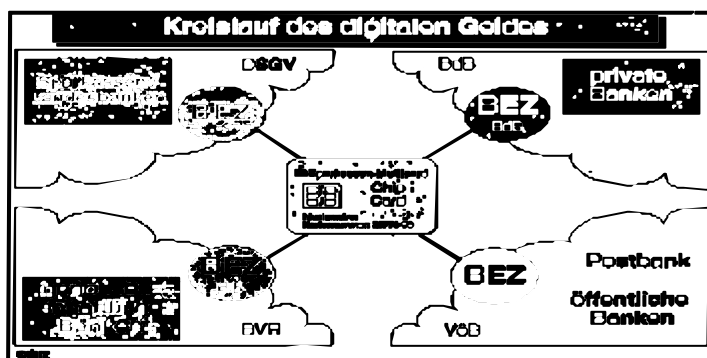
Nr. 3 März 1996

Smartcard bietet vierversprechende Optionen

Im Januar 1996 beginnt ¹ der Chipkarten-Feldversuch des Zentralen Kreditausschusses (ZKA) in den Städten Ravensburg und Weingarten. Die Sparkassenorganisation wird unter Federführung des **SIZ** bis dahin eine Evidenzzentrale aufbauen, die alle eingereichten Zahlungsbeträge der Händler prüft, Gutschriften berechnet, sämtliche Umsätze der Kartenbesitzer zusammenzählt und dem kartenausgebenden Kreditinstitut einmal täglich belastet.

Thomas Krebs, Geldbörsen-Evidenzzentrale

Es hat vergleichsweise lange gedauert, bis sich alle Beteiligten in Deutschland auf einen umfassenden Feldtest mit der multi-



funktionalen Chipkarte geeignet haben. In anderen Ländern - zum Beispiel in Österreich - ist man da schon weiter und bereitet mittlerweile die flächendeckende Ausstattung der Eurocheque-

¹ Der Beitrag entstammt **SIZ Special**, Ausgabe 11/1995. Die, damals noch in die Zukunft sehende, Schreibweise des Artikels wurde nicht verändert, um Verzerrungen des Inhaltes zu vermeiden.

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

Inhalt

Smartcard bietet vierversprechende

<u>Optionen</u>	1
Enorme Vorteile für den Handel	3
Zwei Funktionen auf einer Karte	3
Regionale Interessen	4
Chancen für neue Produkte	5

Offene, nachladbare, elektronische Geldbörsen in Europa

A.) Elektronische Wertkarte und elektronischer Gutschein	6
B.) Elektronische Banknote	7
C.) Elektronisches Bargeld für Dreieckszahlungsvorgang	7
D.) Freies elektronisches Bargeld	7
Ländervergleich in Europa	7
Einige Gedanken zu den Geldbörsenprojekten in Europa	8

Multicard

The next Generation	11
---------------------	----

„ARGE SZS“

Arbeitsgemeinschaft für Sicherheit von Zahlungsverkehrssystemen mit Smart Cards	13
Auftraggeber, Zielsetzung und Aufgabenstellung	13
Hauptaufgaben der ARGE	14
Evaluierung in 4 Stufen	15
Beurteilung des Gesamtsystems	17
Bisherige Erfahrungen	17

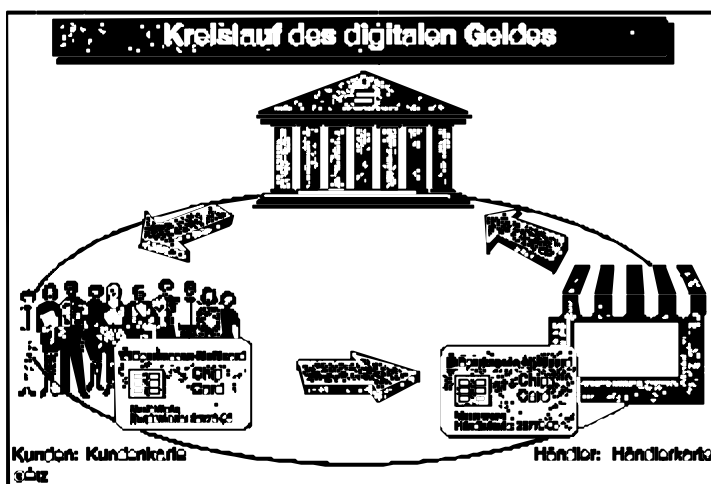
ASA aktiv

<u>Veranstaltungen</u>	18
Konferenzen, Messen	18

Karte mit einem Mikrochip als Zahlungsmittel für kleine Beträge vor. In Deutschland werden ab dem 1. Januar 1996 - so die Planungen - etwa 100.000 Kunden in den Städten Ravensburg und Weingarten die Möglichkeit haben, ihre Rechnungen in Läden, Gaststätten oder in Bussen und Bahnen bargeldlos mit der EC-Karte zu begleichen. Der Zentrale Kreditausschuß (ZKA), in dem die Spitzenverbände der deutschen Kreditwirtschaft zusammenarbeiten, hat diese Region für den Feldtest ausgewählt, weil dort 16 wichtige Kreditinstitute präsent sind und schon heute eine überdurchschnittlich hohe Dichte von Electronic-Cash-Terminals existiert. Die Sparkassenorganisation ist in dem Testgebiet durch die Kreissparkasse Ravensburg und die Landesgirokasse Stuttgart vertreten.

Enorme Vorteile für den Handel

Das Pilotprojekt - dessen Ende noch nicht festgelegt ist - soll Aufschluß über die Akzeptanz der neuen Karte bei Kunden und im Handel geben und die Funktionsfähigkeit der verschiedenen Hard- und Softwarekomponenten in der Praxis erproben. Deshalb kommen auch Mikrochips und Lesegeräte von unterschiedlichen Herstellern zum Einsatz. Verläuft der Feldtest erfolgreich, ist mit einer schnellen bundesweiten Einführung der Smartcard zu rechnen. Bis 1997 - so die Erwartungen - können dann sukzessive rund 35 Millionen EC- und Kundenkarten mit einem multifunktionalen Kleinstcomputer ausgestattet werden. Um die Kompatibilität zu bisherigen Lesegeräten und auch im Ausland sicherzustellen, wird der Magnetstreifen allerdings weiter auf der Karte enthalten sein.



Der integrierte Mikroprozessor bietet jedoch erheblich mehr Sicherheit und eröffnet zahlreiche neue Anwendungsmöglichkeiten für das Plastikkärtchen. Auf den Einzelhandel - der durch die Nutzung des bargeldlosen Weges künftig erhebliche Kosten und Zeit sparen wird - kommt nach den Vorstellungen des ZKA ein "Händlerentgelt" in Höhe von 0,3 Prozent der Verkaufssumme zu, mindestens aber 5 Pfennig pro Transaktion. Diese Regelung wird von den Handelsgruppen derzeit allerdings teilweise noch kritisch betrachtet. Der Vorteil für den Handel ist jedoch immens: Die Abwicklung eines Bezahlvorgangs wird

mit der neuen Karte deutlich schneller, die Wartezeiten an den Kassen kürzer. Hinzu kommt, daß Fehler bei der Wechselgeldausgabe eliminiert werden, Zahlungen mit Falschgeld gänzlich ausgeschlossen sind und sich langfristig der Umgang mit Banknoten und Münzen sowie die damit verbundenen Risiken reduzieren. Das alles erhöht die Zufriedenheit der Mitarbeiter und Kunden.

Mit dem innovativen System können nun auch Zahlungen an Akzeptanzstellen vorgenommen werden, die für Kreditkarten und Electronic Cash nicht in Frage kommen. Das gilt auch für Verkaufsstellen mit relativ geringen Durchschnittsumsätzen sowie für Zigaretten- oder Fahrsccheinautomaten. Das aufwendige und teure Bargeld-Handling entfällt, die Gefahr der Beraubung wird erheblich geringer oder ist sogar vollständig auszuschließen.

Zwei Funktionen auf einer Karte

Die neue Chipkarte verfügt über zwei Funktionen: Electronic-Cash-Offline und elektronische Geldbörse. Da die Persönliche Identifikations Nummer (PIN) und der Verfügungsrahmen zukünftig durch einen Dialog zwischen dem Chip und dem Lesegerät geprüft werden können, ist eine sofortige Authorisierung möglich. Erst wenn der Verfügungsrahmen abgebaut wurde oder eine Überschreitung des Maximallimits von 1.000 Mark erfolgt ist, wird - wie beim bisherigen Electronic Cash-Verfahren auch - eine Online-Überprüfung vorgenommen und der

Verfügungsrahmen wieder auf 1.000 Mark aufgefüllt. Neben der beschleunigten Abwicklung, die besonders für den Lebensmitteleinzelhandel von großem Interesse ist, spart der Handel auch beträchtliche Telekommunikationskosten ein. Diese betragen zur Zeit umsatzabhängig zwischen 0,7 und 0,8 Prozent. Prognosen gehen von einer Reduzierung der Online-Vorgänge um bis zu 95 Prozent durch die neue Electronic-Cash-Offline-Variante und die elektronische Börse aus.

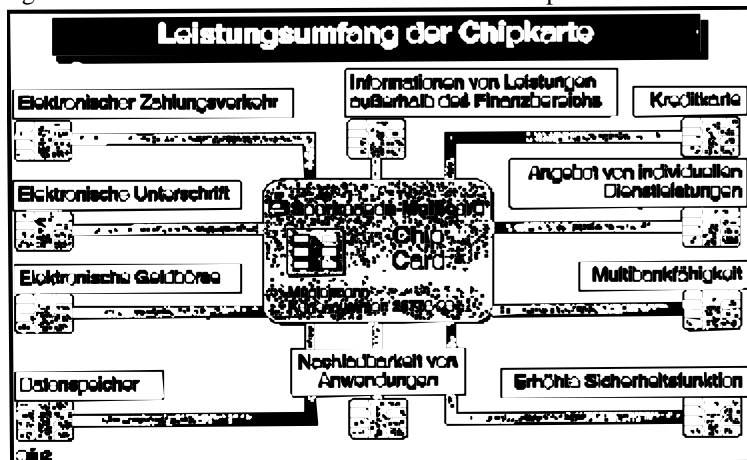
Bei der zweiten Funktion der Smartcard - der elektronischen Geldbörse - handelt es sich um ein völlig neues Produkt. Es wird unter dem Systemnamen "Geldkarte" angeboten. Das virtuelle Portemonnaie ist vor allem für die Begleichung von Kleinstbeträgen zwischen 5 und 25 Mark gedacht. Der Karteninhaber kann dazu an einem Ladeterminal - zum Beispiel einem erweiterten Geldausgabeautomaten - zu Lasten seines Girokontos die Geldbörse mit einem Betrag von bis zu maximal 400 Mark aufladen.

Der geladene Betrag wird einem Börsenverrechnungskonto des kartenausgebenden Instituts gutgeschrieben und einer Börsenevidenzzentrale gemeldet. Deren Aufgabe ist es unter anderem, für jede Karte einen sogenannten "Schattensaldo" zu führen, der durch Aufladungsbeträge angehoben und durch Verfügungsbeträge reduziert wird. Diese Konstruktion ermöglicht es, eventuelle Manipulationen des Systems schnell zu entdecken und im Falle einer Beschädigung von Karten das noch vorhandene Guthaben zu erstatten. Die bargeldlose Bezahlung erfolgt anonym und ohne die Eingabe der Geheimzahl an einem Terminal im Geschäft oder an entsprechend ausgerüsteten Automaten. Jeder Buchungsvorgang reduziert dabei das gespeicherte Guthaben auf der Karte. Die zur Belastung des Börsenverrechnungskontos und zur Gutschrift auf das Händlerkonto notwendigen Daten werden unter Steuerung eines Sicherheitsmoduls - der sogenannten "Händlerkarte" - in den Datenspeicher des Terminals übertragen.

Die in den Lesegeräten so erfaßten Zahlungsbeträge werden vom Händler regelmäßig an eine Händlerevidenzzentrale übertragen, die von der jeweiligen Hausbank vermittelt wird. Diese prüft die Einreichungen, berechnet die Gutschrift für den Händler und leitet die Umsätze an die jeweiligen Kartenevidenzzentralen weiter. Dort werden die Umsätze gegen die Schattenseiten geprüft, anschließend aggregiert und täglich zu Lasten der einzelnen Börsenverrechnungskonten verbucht. Neben der Ausstattung der S-Card (ec) und der S-Card mit der Funktion einer elektronischen Geldbörse ist auch die Ausgabe von Wertkonten als einer anonyme ("weiße") Karte ohne direkten Kontobezug geplant. Sie wird gegen Bargeld oder durch Beteiligung einer zweiten Karte mit Kontobezug mit einem Guthaben geladen.

Regionale Interessen berücksichtigt

Das Informatikzentrum der Sparkassenorganisation hat sich von Anfang an aktiv an der Vorbereitung des Feldtests in Ravensburg/Weingarten beteiligt. Seinem Einsatz ist es unter anderem zu verdanken, daß die regionalen Interessen und Besonderheiten der Sparkassen und Landesbanken/Girozentralen in den ZKA



eingbracht wurden. Dies hat eine erhebliche strategische Bedeutung, denn dadurch wird die Entwicklung regional unterschiedlicher Angebote und Produkte rund um die elektronische Geldbörse möglich.

Das Engagement des SIZ sicherte auch die flächendeckende Portierbarkeit einmal entwickelter Softwarelösungen für die künftigen Börsenevidenzzentralen in den einzelnen Rechenzentren. Am Pilotprojekt in Baden-Württemberg ist neben dem RWSO Stuttgart/Karlsruhe als Verbandsrechenzentrum und der Landes-

girokasse Stuttgart auch die BWS in Münster beteiligt. Sie stellt stellvertretend für die Sparkassenorganisation

die erforderliche Software für die Börsenevidenzzentrale bereit. Das **SIZ** koordiniert diese Entwicklungsarbeiten, übernimmt die Finanzierung und sorgt für den notwendigen Informationsfluß zwischen den Beteiligten und dem ZKA. Die Koordination der Abnahme und Tests der Programme, die Qualitätssicherung sowie die spätere Portierung zählen ebenfalls zu seinen Aufgaben. Dazu gehört auch die Erarbeitung von Konzepten zur Einbindung weiterer Terminals bis hin zur Möglichkeit, die Karte via Homebanking laden zu können. Nach einer Testphase im November erfolgt die gemeinsame Abnahme von Hard- und Software durch den ZKA und im Dezember die Installation der Terminals im Testgebiet.

Chancen für neue Produkte

Für die Sparkassenorganisation wird es entscheidend darauf ankommen, wie sie den Nutzen des neuen Chipkartensystems ihren Privat- und Geschäftskunden deutlich machen kann. Denn im Zuge des härter werdenden Wettbewerbs um den Kartenmarkt versuchen alle Institute, einen "geschlossenen Kreislauf" des digitalen Geldes herzustellen und ihre Terminals an die Händler und ihre Karten an den Verbraucher zu bringen. Mit der Geldkarte eröffnet sich für die Sparkassenorganisation eine vielversprechende Option, ihre Position als Marktführer im Kartengeschäft zu festigen, da ihr alle Vorteile des neuen Zahlungsmittels in besonderem Maße zugute kommen. Dies ist zum einen der Imagegewinn als Anbieter von bequemen und innovativen Finanzdienstleistungen. Zum anderen aber auch die Möglichkeit, Kosten im Bargeldbereich zu senken und neue Einnahmequellen zu erschließen. Dies können z.B. die Karten- oder Transaktionsgebühren für die Händler oder Ladegebühren für Kunden sein.

Da mit einer Ladegebührenregelung ähnlich der des Heimatsparkassenmodells zu rechnen ist - das heißt, das Aufladen der Geldbörse bei Sparkassen ist kostenlos oder zumindest billiger als an Terminals von anderen Instituten - werden die Sparkassen aufgrund der Größe ihres Filialnetzes und der daraus folgenden Dichte an Ladestationen dem Kunden eine besonders bequeme Möglichkeit zur Auffrischung seines Chip-Guthabens bieten. Daraus ergibt sich die Chance einer höheren Kundenbindung.

Mit der "weißen" Karte kann zusätzlich speziell der Jugendmarkt bedient und wirksam konkurrierenden Konzepten aus dem Nichtbankenbereich begegnet werden. Auch eine Nutzung der Smartcard als Telefonkarte ist denkbar. Im **SIZ** stellt man bereits Überlegungen an, wie die örtlichen Stadt- und Kreissparkassen mit Hilfe der elektronischen Geldbörse zusätzliche Dienstleistungen anbieten können. Denn der Mikrochip hat durchaus noch eine Menge Platz zur Speicherung von weiteren Informationen. So könnte zum Beispiel gemeinsam mit den regionalen Verkehrsbetrieben ein System entwickelt werden, in dem die Karte als elektronischer Fahrschein eingesetzt wird. Ähnliches ist mit Sportvereinen oder Kultureinrichtungen denkbar - die EC-Karte mit Chip würde hier als Eintrittskarte für das Fußballstadion, das Schwimmbad, den Skilift, das Museum oder den Zoo dienen.

Natürlich darf bei diesen Zusatzfunktionen das Sicherheitssystem der Karte nicht tangiert werden, dies erfordert erhebliche kryptografische Anstrengungen. Ebenso sind neue Möglichkeiten des Kartenmanagements zu entwickeln. Gemeinsam mit seinen Partnern aus den Entwicklungseinheiten will das **SIZ** in den nächsten Monaten als Know-How-Träger die technischen und organisatorischen Voraussetzungen dafür schaffen, damit alle interessierten Institute in der Sparkassenorganisation die Möglichkeiten des digitalen Zahlungsmittels optimal nutzen und als erste mit neuen innovativen Produkten auf den Markt kommen können.

- Thomas Krebs - Bereichsleiter des Informatikzentrums der Sparkassenorganisation (**SIZ**) in Bonn - ◆

Offene, nachladbare, elektronische Geldbörsen in Europa

In der Urzeit des „Zahlungsverkehrs“ wurden Waren getauscht. Das war etwas umständlich, ganz abgesehen davon, daß man nie genau wußte, ob der andere gerade das brauchte, was man selbst anzubieten hatte. Es folgten "vormünzliche" Zahlungsmittel wie Kaurischnecken und bunte Glasperlen, die alten Römer gossen Kupferplatten mit einem abgebildeten Rind und in reicheren Ländern verwendete man Goldklümpchen, die man abwog. Das Abwägen war umständlich und so entstanden in Kleinasien die ersten geprägten Münzen, die ebenfalls aus Gold waren. Aus dem Namen Moneta der alten Römer entstanden die Namen Münze, money, monnaie, mynt, etc. Für größere Beträge entstanden später noch die Banknoten. Die Entwicklung ging weiter, die wesentlichen Nachteile der Münzen und Banknoten (siehe unten) blieben aber bis heute, über tausend Jahre später, erhalten. Es wechseln heute in Österreich im Gegenwert von rund fünf Milliarden Schilling als Banknoten und rund 230 Millionen Schilling an Münzen täglich den Besitzer. Unter diesem gewaltigen Bargeldberg leiden Kunden, Handel und Geldinstitute.

Der erste Schritt zum elektronischen Bargeld und damit zur Lösung vieler Probleme wurde mit der Entwicklung der elektronischen Wertkarten getan. Diese sind heute in erster Linie in rund einer Milliarde Stück in Form von Telefonwertkarten, meist mit einem einfachen Chip ausgestattet, in über fünfzig Ländern der Welt im Einsatz. Die ersten echten, offenen, nachladbaren, elektronischen Geldbörsen wurden in diversen Pilotprojekten ab Ende der achtziger Jahre getestet. Das erste Land mit einer landesweiten Ausgabe ist Österreich. Manchmal nehmen historische Umwälzungen ihren Anfang an unscheinbaren Plätzen, fernab der Großstädte und Machtzentren. Ein solcher Ort ist Eisenstadt. Dort war die Geburtsstunde der ersten, offenen, multifunktionalen, nachladbaren, elektronischen Geldbörse. Es war der Beginn einer Revolution im Zahlungsverkehr, eines Zeitalters ohne zeitaufwendige und lästige Münzenklauberei, ohne abgezähltes Geld bereitzuhalten, ohne Retourgeld, ohne ausgebeulte Portemonnaies, ohne aufwendige und gefährliche Geldtransporte, ohne Automaten-Plünderer (und damit auch weniger zerstörte Automaten) und mit einem wesentlich veränderten Wertempfinden, der Protokollierung der letzten Ladungen und Bezahlungen (in Österreich je 8), der Sperrmöglichkeit der eigenen Geldbörse und der Möglichkeit einer Vielzahl von Zusatzanwendungen.

Wie funktionieren nun diese elektronische Geldbörsen? Wie unterscheiden sich die verschiedenen Systeme in Europa? Ich möchte in diesem Artikel eine einfache Klassifizierung der Systeme und einen Europavergleich durchführen und dabei auf technische Aspekte verzichten. Wie elektronische Geldbörsen technisch funktionieren, möchte ich in einem Artikel in einer der nächsten Ausgaben der ASA-News behandeln.

Elektronische Geldbörsen kann man nach vielen Gesichtspunkten klassifizieren. Nachfolgend erfolgt eine einfache Einteilung in 4 Klassen (Modelle), wobei das erste Modell, die elektronische Wertkarte, nur eine Vorstufe (ohne „Geld“) darstellt.

A.) Elektronische Wertkarte und elektronischer Gutschein

Beim Wertkartenmodell werden auf die Chipkarten „Werteinheiten“ geladen. Beim elektronischen Gutschein stellen diese Werteinheiten ausgewählte Gutscheine dar. Der Kunde gibt beim Bezahlungsvorgang Werteinheiten (bzw. Gutscheine) nach und nach aus, bis diese aufgebraucht sind. Es erfolgt kein geschlossener Geldkreislauf, die Werteinheiten auf der Chipkarte werden beim Bezahlungsvorgang vernichtet. Dieses Modell

erlaubt eine Anonymität und benötigt nur Billigchips, es ist aber inflexibel, unsicher, nicht offen (für beliebige Händler) und, wenn auf die Chipkarten Werteinheiten nicht nachgeladen werden können (was üblich ist), insgesamt sehr teuer.

B.) Elektronische Banknote

Bei diesem Modell werden heutige Münzen bzw. Banknoten elektronisch nachgebildet. Es werden beim Bezahlungsvorgang dann derartige elektronische Banknoten übertragen, ebenso das Restgeld (elektronische Banknoten sind wie herkömmliches Bargeld nicht teilbar). Die Probleme bei diesem Modell sind die Verhinderung von Kopien von elektronischen Banknoten und die großen Anforderungen an die Chipkarte.

C.) Elektronisches Bargeld für Dreieckszahlungsvorgang

Es erfolgt ein Geldfluß durch kryptografisch gesicherte, elektronische Transaktionen zwischen „Zahler“ und „Empfänger“. Bei diesem Modell ist aber nur ein Geldfluß im Dreiecksverhältnis „Geldinstitut zu Karteninhaber zu Waren-/Dienstleistungsanbieter zu Geldinstitut“ möglich. Es kann in einem offenen System mit beliebigen Organisationen und Branchen eingesetzt werden. Es muß in der Implementierung äußerst sicher sein, vor allem wenn es landesweit wie Bargeld eingesetzt werden soll. Das Modell unterscheidet zwischen Implementierungen mit Transfer von Einzeltransaktionen und Implementierungen ohne Transfer von Einzeltransaktionen (d.h. nur Summentransaktionen) zum Geldinstitut (bzw. zur Verarbeitungsstelle). Mit Summentransaktionen ist es wesentlich wirtschaftlicher und absolut anonym. Bei der österreichischen QUICK-Geldbörse sind zur Einreichung nur Summentransaktionen erforderlich, die Geldbörse in Deutschland benötigt alle Einzeltransaktionen.

D.) Freies elektronisches Bargeld

Dieses Modell entspricht dem letztgenannten, nur besteht keine Einschränkung im Geldfluß. Es erlaubt einen dem heutigen Bargeld vergleichbaren freien Geldfluß (d.h. auch zwischen 2 Karteninhabern). Dieses Modell wurde im Mondex-System realisiert (siehe unten).

Bei allen elektronischen Geldbörsen ist wichtig, daß sie nur unter der Kontrolle der jeweiligen Notenbank und nur von Geldinstituten ausgegeben werden dürfen. Dies ist vor allem aus Gründen der Sicherheit des Zahlungsverkehrs, der Geldmengensteuerung, des Konsumentenschutzes und des Vertrauens der Konsumenten und der Waren- und Dienstleistungsanbieter in das Zahlungsmittel erforderlich. Diese Forderung wird besonders interessant, wenn sich zum Beispiel ausländische Systeme (wie z.B. Mondex) nach Österreich ausdehnen oder wenn weltweit agierende Kreditkartenunternehmen auf ihre Kreditkarten einen Chip mit einer „international verwendbaren“ Geldbörse aufbringen.

Ländervergleich in Europa

Nachfolgend werden die wichtigsten europäischen elektronischen Geldbörsen-Systeme verglichen, wobei nur offene, nachladbare, elektronische Systeme behandelt werden.

Land	Bezeichnung	Kartenanzahl	Maximaler Betrag öS	Infrastruktur	Modell, siehe unten	Multifunktionalität
Österreich	QUICK	2.500.000	1.999	im Aufbau	1,4	ja
Dänemark	DANMONT	300.000	ca. 3.500	gut	1	nein
Belgien	PROTON	24.000	ca. 1.600	im Aufbau	1	nein
Deutschland	Geldkarte	Start 04/96	ca. 2.800	Pilotort	1,3	Ja
Spanien	SEMP	70.000	frei	Pilotinstall.	1	nein
Holland	Chip Knip	100.000	ca. 900	Pilotort	1	nein
Portugal	PMB	700.000	ca. 200	im Aufbau	1	nein
England	MONDEX	40.000	frei	Pilotort	2	nein
Finnland	AVANT	11.000	ca. 1.800	im Aufbau	1	nein
EPI	EXPRESS	Start 1997/98		keine	1,3	nein

EPI (Europay International) ist ein Tochterunternehmen praktisch aller wichtigen Geldinstitute in Europa mit Sitz in Waterloo bei Brüssel. Das PROTON-System (siehe oben) geht in Kürze von der Pilotinstallation in landesweite Einführungen. Das Chipkartenmutterland Frankreich hat die elektronischen Geldbörsenentwicklungen etwas verschlafen (darf aber in Zukunft nicht unterschätzt werden).

Legende zu „Modell“:

1. Elektronische Geldbörse mit Dreieckszahlungsvorgang (siehe oben C.)
2. Freie elektronische Geldbörsen (siehe oben D.)
3. Es werden im System alle Einzeltransaktionen benötigt (siehe oben C.)
4. Alle Terminals können gleichzeitig mehrere Geldbörsensysteme unterstützen

Einige Gedanken zu den Geldbörsenprojekten in Europa

Die Einführung von offenen, landesweiten, elektronischen Geldbörsen in Europa verläuft in den einzelnen Ländern auf sehr ähnliche Art und Weise ab. Es beginnt mit einem Feldtest (eventuell auch zwei) in einer Stadt (oder Region) mit einem eigenen, proprietären System (siehe Tabelle oben). Viele dieser Geldbörsensysteme, so auch die österreichische QUICK-Geldbörse, orientieren sich an dem europäischen Standardisierungsvorschlag CEN 1546, sie unterscheiden sich trotzdem in einigen wichtigen Punkten sehr wesentlich. Neben diesen vielen unterschiedlichen Systemen der einzelnen europäischen Länder versuchen drei Organisationen ein „europäisches System“ anzubieten:

- MONDEX (National Westminster Bank, England)
- CAFE (Entwicklungsprojekt der EU, Brüssel)
- EXPRESS (EPI, Waterloo/Brüssel und Mastercard, USA)

Diese Systeme orientieren sich interessanterweise nicht an dem europäischen Normungsvorschlag der CEN.

MONDEX kämpft mit einem enormen Marketingeinsatz, wie sich bisher zeigt ohne Erfolg. Eine große, international operierende Organisation (den Namen darf ich nicht nennen) interessiert sich aber derzeit für MONDEX. Das Konzept von MONDEX ist für viele Geldinstitute nicht akzeptabel, noch unausgereift und sicherheitstechnisch mit dem heutigen Chipangebot für landesweite Systeme zu unsicher oder zu teuer. Es ist ein interessantes Konzept mit einigen Ideen, die man in Zukunft in einem europäischen System berücksichtigen sollte.

Dasselbe gilt für das CAFE-System, das durch den mächtigen Förderer EU auch einige kleinere Erfolge feiern wird. Zum europäischen System wird sich das CAFE-System ebenso wenig entwickeln wie das MONDEX-System oder irgend ein nationales europäisches System.

Der große Sieger in Europa könnte langfristig das EXPRESS-System sein. Die Entwicklung von EPI (Europay International) und Mastercard, an deren Basisarbeiten (EMV-Standard) auch VISA eine große Rolle spielte, hat auf Grund des enormen Einflusses von EPI sicher die besten Chancen für ein europäisches System. EPI, Mastercard und VISA haben aber zu spät begonnen und waren bei ihren Entwicklungen zu langsam und zu uneinig. Sie konnten daher in den letzten Jahren die vielen landesspezifischen Entwicklungen nicht verhindern. Die Meinungsverschiedenheiten von EPI, Mastercard und VISA führten schon dazu, daß sich VISA abgekoppelt hat und auch zwischen EPI und Mastercard nimmt die Uneinigkeit zu.

Danmont in Dänemark mit der „DANCOIN-Geldbörse“, Banksys in Belgien mit der „PROTON-Geldbörse“, Europay Austria / Austria Card in Österreich mit der „QUICK-Geldbörse“, ZKA (Zentraler Kreditausschuß) in Deutschland mit der „GELDKARTE“, etc., etc., haben ihr eigenes Geldbörsen-System eingeführt (zumindest Pilotprojekte gestartet), sind von ihrem System überzeugt, haben viel Geld investiert und denken nicht im geringsten daran, alles über Bord zu werfen. Die Einführung von offenen, nachladbaren, elektronischen Geldbörsen geht in vielen europäischen Ländern zügig voran und kein MONDEX, CAFE, EXPRESS kann sie stoppen.

Diese Entwicklung in Europa ist für den Kunden sicher nicht zufriedenstellend, er möchte seine Geldbörse in Zukunft auch grenzüberschreitend einsetzen und im Ausland aufladen wollen. Diese Geldbörse soll, wenn möglich, nur einen Geldbörsenspeicher (nur eine Währung) enthalten, weil mehrere Geldbörsenspeicher bei einer Karte ohne Bildschirm für den Kunden zu unübersichtlich und ein Bodensatz in mehreren Währungen für den Kunden nachteilig sind.

Ein europäisches Geldbörsensystem sollte nach meiner Meinung unter anderem mindestens folgende Anforderungen erfüllen:

- Einhaltung aller ISO 7816 Standards, der EMV-Spezifikationen und des CEN 1546 Normungsvorschlages;
- Unterstützung von nur einer Währung (heute die jeweilige Landeswährung des Geldbörsenherausgebers, in Zukunft den EURO);
- Benutzungsmöglichkeit der Geldbörse in allen europäischen Ländern (die Währungskonvertierung erfolgt im Terminal);
- der Bodensatz sollte auch im internationalen Einsatz beim Börsenherausgeber bleiben;
- es sollte kein zentraler Betreiber erforderlich sein;
- jedes Land kann sein nationales Geldbörsensystem nach seinen Bedürfnissen realisieren und betreiben und kann auch zusätzliche Anwendungen mitanbieten, das nationale Geldbörsensystem muß nur kompatibel zum europäischen System sein und ein vorgegebenes, sehr hohes Mindestmaß an Sicherheit erfüllen;
- alle Geldbörsensysteme müssen von ausgewählten Stellen abgenommen werden (nationale Notenbanken, europäisches Währungsinstitut, EPI, etc.), insbesondere hinsichtlich der Funktionalität und Sicherheit.

Viele der heute in Europa am Markt befindlichen Systeme könnten mit mehr oder weniger Korrekturen zu einem europäischen System mit Einhaltung der oben angegebenen Anforderungen zusammengeführt werden, Voraussetzung dazu wäre aber, daß man miteinander spricht, zu Kompromissen bereit ist und dieses europäische Ziel wirklich erreichen möchte.

Weder EPI, noch die Betreiber der einzelnen Landessysteme sind dazu heute bereit. Die meisten möchten bei ihrem eigenen System bleiben und sind damit zufrieden, einige möchten ihre Lösung zur europäischen machen, sie werden dabei aber erfolglos bleiben. Europay Austria und Austria Card haben mehrfach mit einigem Aufwand versucht, mit anderen Anbietern zu kooperieren, es war aber nicht einmal mit unseren Nachbarn Deutschland, der Schweiz und der Tschechischen Republik möglich, eine Annäherung zu erreichen.

Außer viel Lärm von MONDEX und den ersten Prototypen einer mit den einzelnen Ländern nicht abgestimmten EXPRESS-Geldbörse von EPI ist leider vorerst nichts europäisches zu sehen. EPI beginnt aber schon mit den Muskeln zu spielen und wird im Juni 1996 mit einer Marketingoffensive starten. Obwohl die EXPRESS-Geldbörse noch technisch unausgereift ist, spezielle Chips (Chips mit Coprozessor für asymmetrische Kryptografie) erfordert, die heute noch für eine landesweite Einführung viel zu teuer sind und alle

Einzeltransaktionen erforderlich sind (wie beim deutschen System), geben schon einzelne europäische Länder ihre Absichtserklärung ab, mit der EXPRESS-Geldbörse in den nächsten Jahren zu starten.

Wir in Österreich haben, wie die Deutschen, Dänen, Belgier, etc., noch Zeit, etwa 3 bis 5 Jahre. In dieser Zeit muß eine ausreichende Infrastruktur zum Laden und Bezahlen aufgebaut werden und die Bürger und Waren- und Dienstleistungsanbieter müssen zur elektronischen Geldbörse herangeführt, von ihren Vorteilen überzeugt werden.

Die Einführung der elektronischen Geldbörse nur in Form einer eigenen Geldbörsenkarte, wie in Dänemark, Finnland und vielen anderen Ländern, erwies sich als langwierig. Österreich versucht es daher mit einem breiten Angebot mit ec-Karte, Bankkundenkarte, multifunktionaler Geldbörsenkarte (Affinity-Karte) und reiner Geldbörsenkarte. Der Kunde erhält in Österreich eine multifunktionale eurocheque-Karte bzw. multifunktionale Bankkundenkarte mit Chip, der im reinen Offline-Modus die elektronische Geldbörse und Debitfunktion (electronic cash) harmonisch abgestimmt realisiert und zusätzlich im Online-Modus die Geldaufladeautomaten und Online-electronic-cash-Terminals unterstützt. Damit kann mit derselben Karte, je nach Betragshöhe, Anwendungsbereich und Branche die ideale Zahlungsform für den Kunden gewählt werden. Der Kunde wird so schrittweise an die Geldbörse herangeführt, er kann sich langsam an sie gewöhnen. Wenn der Kunde von der elektronischen Geldbörse einmal überzeugt ist (was bis Ende dieses Jahrzehnts in den einzelnen Ländern Europas getrennt gelingen wird), wird er sie in ganz Europa anwenden wollen und spätestens dann ist ein europäisches System gefragt.

Wenn sich bis dahin die EXPRESS-Geldbörse zur europäischen Geldbörse entwickelt hat, wird man wahrscheinlich auch in Österreich zur EXPRESS-Geldbörse wechseln. Dies ist, nach dem heutigen Stand von EXPRESS, auf eine Art und Weise möglich, daß der Kunde nichts davon merkt (außer daß seine neue Geldbörse europaweit funktioniert) und auch die aufgebaute Infrastruktur zum Laden und Bezahlen nur eine neue Software benötigt. Spätestens wenn die europäische Währung EURO eingeführt wird, sollte dieses Szenarium ablaufen. Die bis dahin getätigten hohen Investitionen in die eigenen Geldbörsenprojekte sind in den einzelnen Ländern auf alle Fälle gut angelegt und sie müssen eine wichtige Basisarbeit leisten (den Aufbau einer umfangreichen Infrastruktur und einer Akzeptanz bei den Bürgern und Waren- und Dienstleistungsanbietern).

Wenn es bis dahin keine europäische Lösung gibt und zusätzlich noch internationale Systeme (von EPI, VISA, etc.) dazukommen, hat Österreich derzeit als einziges Land schon in allen Terminals dafür Vorkehrungen getroffen. Die Terminals müssen in Österreich intern vier Kartenleser für Terminalkarten enthalten und mehrere Geldbörsen-Systeme gleichzeitig verarbeiten können. Damit können bei Bedarf schon heute nach einer entsprechenden Vorbereitungszeit mit zusätzlicher Software z. B. das österreichische System und deutsche System gleichzeitig betrieben werden, später einmal z.B. unsere QUICK-Geldbörse gemeinsam mit der EPI- und VISA-Geldbörse. Das österreichische Konzept hat alle diese möglichen Szenarien berücksichtigt.

- Univ.-Doz. Dr. Ernst Piller - Austria Card



Multicard

The next Generation

Die Chipkarte hat in den letzten Jahren einen enormen Aufschwung erlebt, der vor allem in Europa durch den Einsatz als Telefonwertkarte und Krankenversicherungskarte hervorgerufen wurde. Durch unzählige Diskussionen, Ausstellungen, Veröffentlichungen und auch durch die vielen laufenden und abgeschlossenen Feldversuche wurden neue Anwendungsgebiete für den Einsatz der Chipkarten erschlossen. Durch den erfolgreichen Einsatz in vielen Bereichen blieb die Akzeptanz seitens der Anwender natürlich nicht aus. Auch in Österreich hat die Chipkarte mit Anfang dieses Jahres großflächig als Elektronische Geldbörse und Bankomatkarte Fuß gefaßt.

Jeder Anwender kennt die Karte mit dem goldenen Quadrat, das die Chipkarte eindeutig als kontaktbehaftete Chipkarte ausweist. Diese Karte muß lagerichtig in das Schreib/Lesegerät eingesteckt werden, sonst funktioniert sie nicht. Metallstifte kontaktieren die Karte, der Mikrochip wird mit Spannung versorgt und die erforderlichen Transaktionen können abgewickelt werden.

Auf den ersten Blick erscheinen die kontaktbehafteten Karten für alle derzeitigen Anwendungsbereiche ausreichend. Gestiegene Anforderungen an die Benutzerfreundlichkeit, die Umweltbeständigkeit, Datensicherheit und an den Schutz vor Vandalismus waren der Auslöser für die Entwicklung der nächsten Generation von Chipkarten, der Generation der kontaktlosen Chipkarten.

Kontaktlose Chipkarten haben keine nach außen geführten mechanische oder elektrische Kontakte. Durch diese dichte Einbettung des Chips in den Kartenkörper und die rein induktive bzw. kapazitive Daten- und Energiekopplung zwischen Schreib/Lesegerät und der Karte wird bei den kontaktlosen Karten eine hohe Unempfindlichkeit gegenüber Umwelteinflüssen und durch den Wegfall mechanischer Kontakte eine lange Lebensdauer sowie wartungsfreier Betrieb erreicht. Die Datenübertragungsrate sowie die Daten- und Übertragungssicherheit können durch diese Art der Chipeinbettung und der Kopplung wesentlich erhöht werden.

Die bei den kontaktlosen Karten lagenunabhängige Kommunikation, die Karten funktioniert in jeder Lage mit dem Schreib/Lesegerät, ergeben sich für den Kartenbenutzer Bedienungsvorteile. Das umständliche Drehen und Wenden der Karte in die richtige Position fällt bei den kontaktlosen Karten weg.

Diese Eigenschaften und modernste Chiptechnologien machen die kontaktlosen Karten zu Spezialisten für den Einsatz als Multifunktionskarten. Multifunktionskarten können mehrere, durch Kryptographie gesicherte, Anwendungen auf einer Karte verwalten und ablaufen lassen.

Wesentlich für die Funktionalität der Chipkarten ist die Kopplungsentfernung. Drei Systeme, Close Coupling, Proximity und Hands Free, werden unterschieden.

Bei Close Coupling Systemen beträgt die Kopplungsentfernung für die Spannungsversorgung und die Datenübertragung zum Schreib/Lesegerät 0 bis 3 mm. Mit dieser Technik werden die derzeit höchsten Datenübertragungsraten mit bis zu 300 kbit/s Lese- und Schreiboperationen erreicht. Bei den komplexesten Typen erfolgt die Datenübertragung gesichert mit mittels spezieller Protokolle und Verschlüsselungsalgorithmen. Die modernsten Karten, die diese Technologie benutzen, verwenden speziell auf Chipkarten zugeschnittene RISC Prozessoren. Die Schreib/Lesegeräte sind Auflagereader, Geräte mit einer markierten Fläche, auf die die Karte kurz gelegt wird, Muldenreader mit vertieften Ausnehmungen für die Karte oder, bei Verwendung als direkter Ersatz für Magnet- oder kontaktbehaftete Karten, auch die altbekannten Schlitzleser. Typische Anwendungsbereiche sind Telekommunikation, Banking, Sicherheitstechnik, elektronisches Roadpricing und Multiapplikationsanwendungen wie sie bei einer City Card, die mehr als nur Geldbörse ist, auftreten.

Proximity Lösungen arbeiten mit einer Kopplungsentfernung bis maximal 100 mm. Die Karte wird beim Schreib/Lesegerät vorbeigeführt, das Schreib/Lesegerät und die Karte enthalten kleine Antennen. Bei den Schreib/Lesegeräten sind Antennen mit bis zu 300 mm Durchmesser üblich. Mittlere Datenübertragungsraten bis zu 100 kbit/s werden erreicht, die Sicherheit der Datenübertragung und -verarbeitung ist geringer als bei Close Coupling Techniken. Typische Anwendungen fallen in den Bereich Zutrittskontrolle und Ticketing.

Hands Free schließlich bedeutet, wie der Name schon sagt, daß die Karte nicht mehr in die Hände genommen werden muß, um sie zu bedienen. Die Karte kann in der Tasche stecken bleiben da die Kopplungsentfernung

bis zu 1500 mm beträgt. Die Datenübertragungsraten sind gering, die Karten sind mit keiner Sicherheitstechnik und wenig Intelligenz ausgestattet. Es sind nur Leseoperationen von der Karte möglich. Die Anwendungsgebiete sind Identifikationssysteme für zum Beispiel Lager- oder Containerverwaltung sowie für Zutrittssysteme ohne hohe Sicherheitsansprüche.

Wie bei den Kopplungsarten bereit erwähnt bestehen zwischen den einzelnen Kartentypen und Kopplungsarten gravierende Unterschiede bei den verwendeten Chips. Bei den Hands Free und Proximity Lösungen werden sogenannte Low Level Systeme verwendet. Das sind meistens reine Speicherchips, die nur lese- und in den seltensten Fällen auch schreibfähig sind. Diese Speicherkarten besitzen keine Intelligenz, die auf der Karte gespeicherten Daten sind selten gegen Manipulation geschützt.

Die bei manchen High Level Karten verwendeten Materialien entsprechen auch bereits den gestiegenen Anforderungen hinsichtlich Umweltverträglichkeit und Beständigkeit. Kontaktlose Karten aus Polyesterlaminat bleiben von -20 Grad bis zu 110 Grad Celsius funktionsfähig, sind wasserdicht und haben, im Gegensatz zu den herkömmlichen PVC Karten mit geringerer Temperaturbeständigkeit und Lebensdauer, eine Lebensdauer von bis zu 10 Jahren.

Multiapplikationskarten, z.B. City Cards, wie sie den modernsten Anforderungen entsprechen, kombinieren verschiedenste Applikationen wie Ticketing, Elektronische Geldbörse, Ausweise etc. auf einer Karte. Die Karte muß die teilweise konkurrierenden Anwendungen sicherheitstechnisch unter höchstem Datenschutz von einander trennen. Der auf der Karte untergebrachte Mikroprozessor muß ein flexibles Filesystem, ähnlich dem auf einer Festplatte, und diverse Zugriffsberechtigungen auf die verschiedenen Applikationen verwalten können. Verschlüsselte Übertragung sensibler Daten, wie sie bei der Abwicklung eines Zahlungsverkehrs anfallen, höchste Sicherheit bei der Authentifizierung der Kommunikationspartner sind Grundanforderungen an eine kontaktlose Karte, damit diese (daten)sicher als Multiapplikationskarte arbeiten kann und auch gegen betrügerische Attacken gewappnet ist.

Kontaktlose Chipkarten vereinen Bedienerfreundlichkeit, hohe Lebensdauer und Belastbarkeit mit modernster Technologie und werden sicherlich in nächster Zeit die kontaktbehafteten Karten in allen Bereichen ablösen. den betroffenen Betreibern und Herstellern - auch zu ihrem eigenen Nutzen - gefestigt.

- DI. Alexander Zeppelzauer - KAPSCH AG - Abteilung Smart Card Systems - zuständig für Marketing und Product Management - ◆

„ARGE SZS“

Arbeitsgemeinschaft für Sicherheit von Zahlungsverkehrssystemen mit Smart Cards

Aufgrund der Aufgabenstellung seitens des Europäischen Währungsinstituts, die Sicherheit und Akzeptanz von offenen prepaid-card-Systemen zu überwachen, entstand eine Initiative der OeNB, im Rahmen eines Projekts allgemeingültige Aussagen über die Sicherheit von Zahlungssystemen mit Smart Cards, speziell über das österreichische PAYCHIP-System machen zu können.

Unabhängige, kompetente Expertise

Zur Sicherung der Objektivität wurde gefordert, daß die Beurteilung der Systemsicherheit durch unabhängige Experten erfolgen sollte, womit sich eine Konstruktion außerhalb der OeNB und der Betreiberfirma Europay Austria (EPA) anbot. Da es sich um eine abgeschlossene Projektarbeit handelt, wurde die Rechtsform einer ARGE bzw. Gesellschaft nach bürgerlichem Recht gewählt.

Nach Vorarbeiten seit Dezember 1994 wurde die ARGE SZS im Mai 1995 gegründet. Es gelang, für jedes fachliche Themengebiet Experten höchster fachlicher Kompetenz als Mitglieder der ARGE zu gewinnen:

- Univ. Prof. Dipl. Ing. Dr. Dietmar Dietrich, TU Wien
- Dipl. Ing. Dr. jur. Dr. techn. Walter J. Jaburek, ger. beeideter Sachverständiger
- Univ. Prof. Dipl. Ing. Reinhard Posch, TU Graz
- Dr. Peter Rihl, Revidata
- Doz. Dipl. Ing. Dr. Ingrid Schaumüller, Universität Linz
- Dipl. Ing. Erwin Schoitsch, FZ Seibersdorf

Durch die Einbettung in die *STUZZA*² und Nutzung deren Ressourcen konnte der administrative Aufwand so gering als möglich zu halten.

Vertraglich ist für die ARGE - Mitglieder eine Abgrenzung zwischen der Tätigkeit im Rahmen der ARGE und ihres Fachberufes geregelt, insbesondere betreffend möglicher Interessenskonflikte.

Eine Einflußnahme von außen auf die Ressourcenzuteilung innerhalb der ARGE würde die Objektivität und Glaubwürdigkeit der Ergebnisse in Frage stellen und ist daher nicht zulässig.

Abgesehen davon, daß die Mitglieder der ARGE zur Geheimhaltung aller ihnen im Rahmen der ARGE zugänglichen Informationen verpflichtet sind, wird vom Projektmanagement her darauf geachtet, daß möglichst wenig Know-How über ein zu betrachtendes System in operativer Detaillierung aus der Tätigkeit in der ARGE konzentriert wird. Dies gilt für einzelne Mitglieder, Mitarbeiter und die ARGE insgesamt. Daher sollen abgesehen von der Systemkonzeptebene keine Tätigkeiten durch die ARGE erfolgen, die derart detaillierte Informationen erfordern.

Die Verwendung bzw. Einholung von allgemein anwendbarem Wissen (Normen, allgemein angewendete Mechanismen, bekannte Algorithmen, ..) wird nicht beschränkt, da es zur Formulierung von Sicherheitsvorgaben erforderlich ist.

² Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr

Auftraggeber, Zielsetzung und Aufgabenstellung

Sämtliche Aktivitäten der ARGE erfolgen im Auftrag der Oesterreichischen Nationalbank (OeNB). Sie definiert den im Rahmen der ARGE auszuführenden Projektauftrag und dotiert dafür ein Projektbudget und ist über einen fachlichen Vertreter (Dir.Rat Erwin Tischler) in die Projektarbeit eingebunden.

Herzstück des Auftrags ist eine unabhängige Beurteilung der Sicherheitsarchitektur des österreichischen „PAYCHIP“-Systems, (d.h. Einsatz von Chipkarten als Zahlungsinstrumente) durch Experten mit höchster einschlägiger Kompetenz zu erhalten und daraus allgemein gültige Sicherheitsziele für ein offen zugängliches Zahlungssystem mit Smart Cards zu formulieren. Die ARGE ist ausschließlich ihrem Auftraggeber OeNB verantwortlich, fachlich richtige und fundierte Aussagen bzw. Empfehlungen abzugeben. Darunter fallen jedoch nicht Eingriffe in das Design oder die Entwicklung konkreter Systeme. De facto beschränkt sich die ARGE auf die Anwendung der „Elektronischen Geldbörse“, da hier eine neue Technologie zum Einsatz kommt, für die es noch wenig Erfahrung gibt..

Die Hauptaufgaben der ARGE sind:

1) Allgemeingültige Empfehlungen, welche Sicherheitsziele an ein offen zugängliches Zahlungssystem mit Smart Cards zu stellen sind

Diese wurden von der ARGE im Rahmen einer Sicherheitspolitik ausgearbeitet. Sie stellt ein allgemeingültiges Regelwerk auf Top-Level dar, das sich für jedes auf Smart Cards basierende ZV-System anwenden läßt. In der Sicherheitspolitik sind die grundsätzlichen Sicherheitsziele festgelegt, aus denen sich die von einzelnen Subsystemen bzw. Komponenten zu erfüllende Sicherheitsziele ableiten.

Die Systemsicherheitspolitik stellt eine Spezialnorm auf Basis der "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)", EG Juni 1991 dar, wie sie durch die Empfehlung des Rates der Europäischen Union³ zur Anwendung von Sicherheitsanalysen empfohlen wurden.

Die Sicherheitspolitik besteht im wesentlichen aus „obersten Regeln“, der Definition Sicherheitsfunktionalitätsklasse („F-ZS“) sowie einer Evaluierungsstufe („E-ZS“), an der die Vertrauenswürdigkeit der sicherheitstechnischen Einrichtungen gemessen werden kann.

Die obersten Regeln der Sicherheitspolitik sind:

Integrität: Erzeugung, Veränderung und Löschung von Informationen, die Geldbeträge oder Berechtigungen darstellen, darf ausschließlich nach festgelegten Regeln erfolgen.

Beweissicherung: Änderungen von dauerhaften sicherheitsrelevanten Informationen müssen protokolliert und dieses Protokoll solange notwendig sicher aufbewahrt werden.

Verfügbarkeit: Der Systembetrieb muß auch bei Störungen, Zerstörung von STEs und Verlust der Vertraulichkeit bei dezentralen STEs weitergeführt werden können.

Revision: Die Sicherheit des Gesamtsystems ist periodisch einer Revision zu unterziehen.

Diese vier Grundregeln werden gemäß der ITSEC-Norm in einer neu definierten Sicherheitsfunktionalitätsklasse („F-ZS“) konkretisiert und detailliert. Die Neudefinition war notwendig, da sich die vordefinierten Funktionalitätsklassen nur mit einzelnen Komponenten eines EDV-Systems beschäftigen. Ein Zahlungsverkehrssystem stellt demgegenüber ein vernetztes System aus technischen Einrichtungen (TEs) wie zB Karten, Terminals, Buchungszentren und Netzwerkverbindungen, sowie aus organisatorischen und

³ Empfehlung über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik 95/144/EG vom 7.April 1995

kryptographischen Abläufen dar, das in seiner Gesamtheit zu prüfen ist. Als „zu evaluierender Gegenstand (EVG; ITSEC-Diktion) wird daher das gesamte Zahlungsverkehrssystem ZS definiert. A

Sicherheitsstudie

Sie besteht im wesentlichen aus einer Grobevaluierung auf Systemkonzeptebene und soll einen strukturierten Evaluationsplan sowie eine grobe Abschätzung der Angriffs-, und Schwachstellenpotentiale aufzeigen. Die Kernaussage zeigt, ob die Sicherheitsziele laut Sicherheitspolitik vom Zahlungsverkehrssystem in seiner Gesamtheit erfüllt werden können. Diese Grobevaluierung wird für das PAYCHIP System zur Zeit vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn in enger Zusammenarbeit mit den Mitgliedern der ARGE ausgearbeitet.

Aus dem Inhalt:

Abschätzung von Angriffs- und Schwachstellenpotentialen
Abschätzung der Erfüllung der Sicherheitsziele
Anforderungen an Prüfinstanzen für die themenbezogene Evaluierung
Auflistung und Priorisierung der zu evaluierenden Subsysteme und Komponenten
Möglichkeiten und Grenzen der Prüftiefe aufgrund Verfügbarkeit von Unterlagen
Empfehlung an den Auftraggeber, den Nachweis über die Erfüllung der Sicherheitsziele pro sicherheitsrelevantem EVG zu verlangen.

2) Mitwirkung an Detailüberprüfungen von Subsystemen und/oder Komponenten.

Zunächst wurden von der ARGE die sicherheitsrelevanten Prüfobjekte definiert:

Chip-Hardware:

Erfolgreiches Eindringen in den Chip könnte zur Fälschung von Geldbörsenbeträgen oder Transaktionen bzw. Aufdecken geheimer Schlüssel führen

Software:

Manipulierte Chip-, Terminal-, Autorisierungssoftware könnte zu gefälschten Transaktionen oder Aufdecken geheimer Schlüssel führen. Insbesondere ist das Insider-Risiko zu beurteilen.

Initialisierung, Personalisierung:

Bei diesem Vorgang wird mit der Chip-Software und den systemweiten Schlüsseln umgegangen. Sicherheitslücken in diesem Bereich könnten massive Folgerisiken auslösen.

Terminals:

Sie bestehen aus dem (unsicheren) Gerät samt Software und dem eingebauten Sicherheitsmodul. Erfolgreiche Angriffe auf diesen könnten gefälschte Einreichtransaktionen und das Aufdecken systemweiter Schlüssel zur Folge haben. Erschwerend wirkt sich aus, daß die ausgelieferten Terminals nicht kontrolliert werden können.

Pro Prüfobjekt erfolgt die Evaluierung 4 Stufen:

1) Sollvorgabe

Ihr Inhalt leitet sich aus den Sicherheitszielen (laut Sicherheitspolitik) ab. Die Eigenschaften und das Einsatzgebiet des zu untersuchenden Objekts bestimmt die Themenstruktur und -abgrenzung (z.B. ob es sich um eine technische Einrichtung oder einen organisatorischen Vorgang handelt). Einflußfaktoren auf die Untersuchung sind der jeweilige Stand der Technik, anwendbare Normen und Standards sowie bereits bestehende externe Arbeiten.

Als Ergebnis wird ein Katalog von Fragen, Anforderungen und Durchführungsvorschlägen für die Erhebung des Istzustandes (2) geliefert, dessen Detaillierung den nachfolgenden Soll-Ist-Vergleich und daraus resultierende Schlußfolgerungen ermöglicht. Die Ausarbeitung erfolgt auf Initiative der ARGE und kann durch ihre Mitglieder oder eine beauftragte Prüfinstanz erfolgen.

2) Erhebung des Istzustandes

Dies erfolgt aufgrund der Sollvorgabe durch eine Prüfinstanz, welche vom betroffenen Systemhersteller bzw. -betreiber zu beauftragen ist. Die ARGE empfiehlt dabei der OeNB Kriterien für den Inhalt der Erhebung und die Qualifikation der Prüfinstanz. Abhängig vom Prüfgegenstand sind die sicherheitsrelevanten Konzepte und Mechanismen, die verfügbare Dokumentation, die Einhaltung und Abweichung von gängigen Normen, aber auch die Eigenschaften des realen Systems wie seine Funktionalität im Normalbetrieb / unter Ausnahmsbedingungen, seine sicherheitsrelevanten Mechanismen und deren Stärke, sein Verhalten an den Schnittstellen zur Außenwelt zu evaluieren. Schließlich sind auch die Einflüsse des Konstruktions-, Herstellungs- und organisatorischen Umfelds auf die Sicherheit zu untersuchen.

Der abzuliefernde Prüfbericht beschreibt die Erhebungsmethodik und die sicherheitsrelevanten Eigenschaften des Prüfgegenstandes. Die Stärke der Sicherheitsmechanismen muß in ausreichender Detaillierung nachgewiesen werden.

3) Soll- Ist Vergleich

Dieser enthält Aussagen aufgrund der Ergebnisunterlagen der Sollvorgabe und Ist-Erhebung über:

Nicht beantwortete Fragen

Nicht oder teilweise erfüllte Anforderungen

Einhaltung von Normen und Standards

Begründung von Abweichungen

Auswirkungen auf die geforderte Sicherheit in qualitativer bzw. quantitativer Hinsicht.

Analog zur Ist-Erhebung erfolgt die Ausarbeitung durch eine Prüf- oder Evaluierungsinstanz.

4) Schlußfolgerungen

Sie werden aufgrund des Soll-Ist Vergleichs gezogen und stellen eine Beurteilung der Sicherheit des Prüfgegenstandes dar::

Systemimmanente Risiken und im Zuge der Evaluierung erkannte Risiken sowie deren Auswirkungen auf das Gesamtsystem.

Abschätzung, ob und mit welchen Maßnahmen die erkannten Risiken behoben werden können bzw. welches auf den Prüfgegenstand bezogene Restrisiko zu quantifizieren ist.

Diese Schlußfolgerungen können von der beauftragten Prüfinstanz oder aber der ARGE ausgearbeitet werden.

Diese Detailprüfungen werden im Auftrag und auf Kosten der betroffenen Systemhersteller bzw. -betreiber durchgeführt und ihre Ergebnisse von der ARGE beurteilt, wobei eine Empfehlung an die OeNB abgegeben wird.

Beurteilung des Gesamtsystems

Nach Vorliegen aller beschriebenen Studien erfolgt ein Abschlußbericht, mit schlüssigen Aussagen auf Systemebene, ob und inwieweit die Sicherheitsziele von einem konkret betrachteten Zahlungsverkehrssystem erfüllt werden, bzw. welche Ziele nicht erfüllt sind.

Daraus wird geschlossen, welche Restrisiken (soweit möglich, als Geldbeträge quantifiziert) im allgemeinen und aufgrund von erkannten Abweichungen des betrachteten System bestehen. Darüber hinaus werden Vorschläge eingebracht, mit welchen Maßnahmen die Ziele erfüllt werden können und welcher Aufwand dafür notwendig ist.

Die OeNB kann eine positive Empfehlung seitens der ARGE als Voraussetzung für eine völlige bzw. eingeschränkte Systemfreigabe festlegen.

Analog zur derzeitigen Evaluierung des PAYCHIP-Systems ist die Überprüfung von neuen weiteren, auf mit Chips ausgestatteten Karten basierenden Zahlungssystemen bzw. -instrumenten vorgesehen. Das heißt, es wird festgestellt, ob und inwieweit sie den Bedingungen der Sicherheitsstudie zu unterziehen sind und entsprechende Prüfeempfehlungen abgegeben.

Darüber hinaus werden im Rahmen der ARGE Informationen über Arbeitsergebnisse und Entwicklungen in einschlägigen internationalen Prüf- und Normungsgremien aufbereitet.

Zeithorizont

Die ARGE ist nicht als ständige Einrichtung vorgesehen, sondern soll die Kriterien und Grundlagen für Sicherheitsbeurteilungen durch in Zukunft dafür einzurichtende Instanzen schaffen. Daher soll die zuvor beschriebene Evaluierung des Gesamtsystems noch im Jahr 1996 vollständig abgeschlossen und kommuniziert werden.

Bisherige Erfahrungen

Aus eigener Sicht konnte die ARGE inhaltlich ihrem Auftrag entsprechen und bis jetzt einige der geforderten Ergebnisse erfüllen. Mit der Sicherheitspolitik gelang es, eine abstrakte Definition von Sicherheitszielen, die für jedes electronic-purse System anwendbar sind, zu formulieren. Da sich die Forderungen so streng als nur möglich an internationalen Normen orientieren, kann die Sicherheitspolitik zumindest teilweise auch als Vorbild für andere Länder dienen.

Die bisher vorliegenden Empfehlungen bzw. Ergebnisse von Detailprüfungen haben neben ihrem eigentlichen Zweck das Bewußtsein um die Notwendigkeit und Sinnhaftigkeit von externen Sicherheitsuntersuchungen bei den betroffenen Betreibern und Herstellern - auch zu ihrem eigenen Nutzen - gefestigt.

- Manfred Holzbach - Geschäftsführer der ARGE SZS -



ASA aktiv

- Am 24. September 1996 findet die alljährliche ASA Chipkartenkonferenz, diesmal unter dem Motto „Leidensweg - Erfolgserlebnis - Perspektiven“ im Hotel Schloß Wilhelminenberg, A 1160 Wien, Savoyenstraße 2 statt.
Bitte merken Sie diesen Termin vor.
- Konferenz „Bridging the Card Gap“, 18.-19. April 1996, in Wien / Eisenstadt
Achtung ! für ASA Mitglieder gilt bei Anmeldung bis 4.4.1996 die ermäßigte Teilnahmegebühr, siehe auch beiliegender Prospekt !
- Dieser Ausgabe der ASA News liegt der Zahlschein für den Jahresmitgliedsbeitrag bei.
- ASA - Radlwimmer -

Veranstaltungen

Konferenzen, Messen

APRIL 1996

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

Datum	Thema	Veranstalter	Ort
16-17.	Successful Business & Marketing Strategies for Electronic Cash	International Quality & Productivity Centre +44 (0)181 332 1112	London
17-18.	Smart Cards in Transport: Practical Progress and the Way Ahead	International Conference Group +44 (0)181 743 8787	London
18-19.	Bridging the Card Gap *)	Smart Card Forum +49 4131 9834 14	Wien
18-19.	Electronic Cards Payment in Eastern Europe: A Tutorial	IBC Technical Services +44 (0)171 637 4383	Budapest
22.-23.	Electronic Payment Services '96	IBC Technical Services +44 (0)171 637 4383	London

*)

Bridging the Card Gap, 18.-19. April 1996, in Wien / Eisenstadt

Achtung ! für ASA Mitglieder gilt bei Anmeldung bis 4.4.1996 die ermäßigte Teilnahmegebühr, siehe auch beiliegender Prospekt !

MAI 1996

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

Datum Thema
 11.-19. Toward an Electronic Patient Record
 13.-16. CardTech/SecureTech '96

Veranstalter
 MRI
 CTST
 +1 301 881 3383

Ort
 San Diego
 Atlanta

JUNI 1996

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

Datum Thema
 4.-6. Card Australia
 5.-7. 3rd Europay Members Meeting
 25.-26. Chip Cards

Veranstalter
 AIC
 Europay
 IIR
 +43 1 8938346

Ort
 Sydney
 Sevilla
 Wien

SEPTEMBER 1996

Datum Thema
 24. ASA jährliche Konferenz

Veranstalter
 ASA
 +43 1 6151134 751

Ort
 Wien

OKTOBER 1996

Datum Thema
 21.-25. 6th International Manufacturers Association Conference & Exhibition
 29.-31. Cartes '96

Veranstalter
 ICMA
 CEP

Ort
 Bermuda
 Paris