

# ASA NEWS

## Quick und der Euro - eine Erfolgsstory

Nr. 15 Mai 2002

## Inhalt

Mit der **Einführung des Euro als Bargeld** hat Quick rasch an Bedeutung gewonnen. Als kleinster Geldschein



steht die "5 Euro-Banknote" zur Verfügung, wodurch die ehemaligen ATS 50 - bzw. ATS 20 - Banknoten größtenteils durch Zahlungen mit Euro- und Cent-Münzen substituiert werden. Um dem wachsenden Münz volumen zu entgehen, verwenden immer mehr Kunden ihre Elektronische Geldbörse. Auch der seit 1.1.2002 erhöhte Ladebetrag mit maximal € 400,- hat die Attraktivität von Quick weiter erhöht.

In den ersten vier Monaten 2002 wurden **über 6,1 Mio. Quick-Zahlungen** mit einem **Umsatzvolumen von rund € 47 Mio.** durchgeführt.

Der nachfolgende Vergleich des ersten Quartals 2001 zu 2002 zeigt die erfreuliche Entwicklung:

**Quick und der Euro -  
eine Erfolgsstory** 1

*Zahlungsverteilung* 3

*Beispielhafte Anwendungen* 4

*Quick-Ladepromotion* 5

**Multifunktionaler  
Ausweis und  
Elektronische Signatur  
im Unternehmen** 6

*1. Ausgangssituation* 6

*2. Unternehmensausweis* 7

*3. Public Key Infrastructure* 9

*4. Digitale Signatur* 11

*5. Zusammenfassung* 13

**Schaltbare  
Dual-Interface  
SmartCard** 14

*Überblick* 14

*Dual-Interface Chipkarten* 14

*Das Patent* 15

*Serviceverrechnung von  
Verkehrsdienstleistungen* 16

*Zusammenfassung* 17

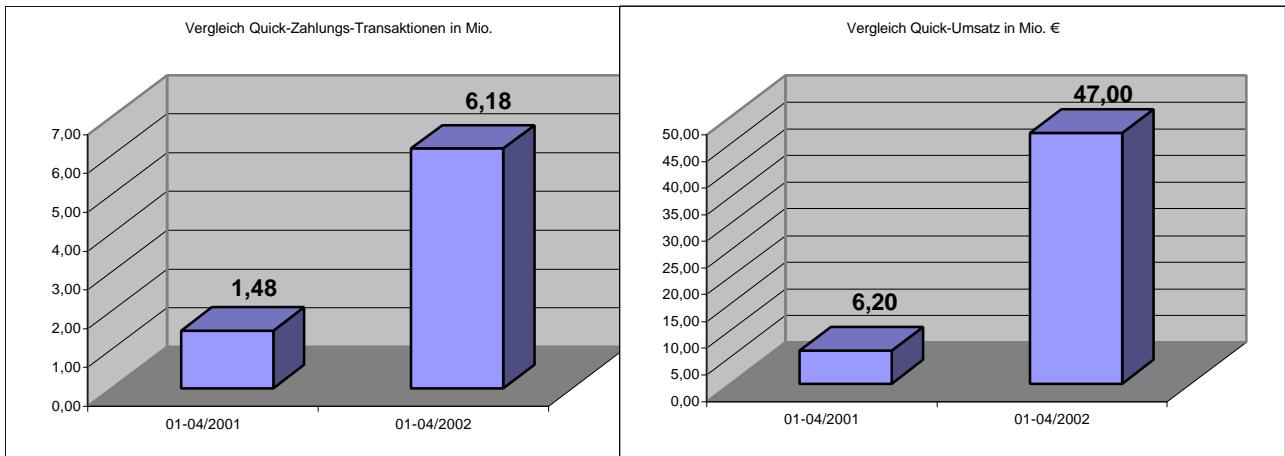
**Veranstaltungen** 18

**ASA Konferenz 2002** 19

*Kontaktlose Chipkarten* 19

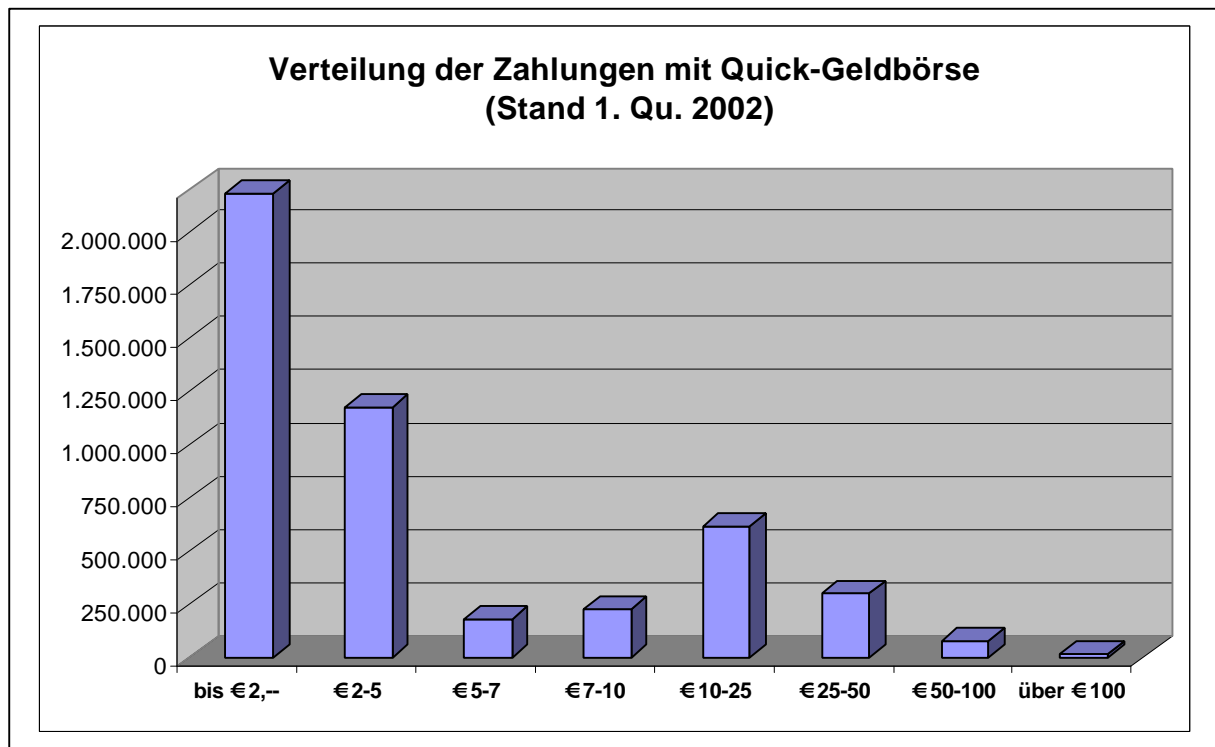
Impressum: Informationsschrift für die Mitglieder der ASA,  
Herausgeber:  
Austrian Smart-Card Association - Österreichische Chipkarten Vereinigung,  
A 1127 Wien, Postfach 81, Tel.: +43 1 899 346 00, FAX: +43 1 899 347 77  
email: asa@ict.tuwien.ac.at, DVR: 0698121  
internet: <http://www.asa.or.at>





Quick befindet sich derzeit auf insgesamt **5,7 Mio. Chipkarten**: Maestro-Karten, Bankkundenkarten mit Chip (ohne Maestro-Funktion), anonymen Quick-Wertkarten u. diversen Quick-Affinitykarten. Voraussetzung für das Zahlen mittels Quick ist das vorherige Laden der Elektronischen Geldbörse (max. € 400,-). Dieser Vorgang kann an **rund 5.600 Ladeterminals** (davon an 2.673 Bankomaten rund um die Uhr) durchgeführt werden. Anschließend kann Quick überall dort zur Zahlung eingesetzt werden, wo das Quick-Logo ersichtlich ist - und zwar in ganz Österreich bei derzeit knapp **70.000 Zahlterminals** (Bankomat-Kassen, Quick-Automatenmodule und Quick-Only-Terminals).

## Zahlungsverteilung



**Kunden** profitieren bei der Verwendung von Quick vor allem von der einfachen Handhabung: bargeldlos Zahlen ohne Code und ohne Unterschrift, lediglich durch Bestätigung des Rechnungsbetrags mittels OK-Taste. Bei Automaten entfällt zusätzlich das lästige Suchen nach dem passenden Kleingeld. Darüber hinaus fällt nur beim Laden, nicht jedoch beim Zahlen, eine Buchungszeile am Kontoauszug an.

**Händler** schätzen die Elektronische Geldbörse aufgrund mehrerer Vorteile, wie z.B. geringere Bargeldmanipulation, weniger Wechselgeld sowie einfache und schnelle Abwicklung von Zahlungen ohne Online-Verbindung. Automatenbetreiber haben zudem ein stark reduziertes Vandalismusrisiko und die Möglichkeit der flexiblen Preisfestsetzung. Die Kosten für die Akzeptanz von Quick fallen mit 0,5% Disagio (bei elektronischer Umsatzeinreichung) zuzüglich Einreichentgelt sehr günstig aus. Anfragen zu den Konditionen, zum Quick-Akzeptanzvertrag bzw. zu den div. Quick-fähigen Terminals können per E-Mail an [verkauf@europay.at](mailto:verkauf@europay.at) bzw. telefonisch an 01-71701-1800 gerichtet werden.

## ***Beispielhafte Anwendungen von Quick***

- Knapp 1.800 Quick-Parkscheinautomaten in 60 Städten und Gemeinden
- An 318 Fahrscheinautomaten kann mit Quick bezahlt werden (davon 240 bei den ÖBB und 78 bei den Linz Linien), weitere Automaten bei den ÖBB und Wiener Linien sind in Vorbereitung
- Über 1.400 Waschmünzzähler mit Quick-Akzeptanz sind in Wohnanlagen in Betrieb
- Mehr als 390 Kopierer sind mit Quick-Modulen ausgestattet
- Bereits über 300 Zigarettenautomaten akzeptieren neben Bargeld auch Quick
- 10 öffentliche Payphones der Telekom Austria im Wiener AKH
- Mehrere große Unternehmen (z.B. AL-KO / Obdach, Bawag / Wien, Blum / Höchst, Eckelt Glas / Steyr, Engel / Schwertberg, Dietach und St. Valentin, Fischer / Ried im Innkreis, GF Fischer / Traisen, Internorm / Sarleinsbach, LKW Walter / Wr. Neudorf, Magna / Ilz, OeNB / Wien, Palfinger / Salzburg, RLB OÖ / Linz, RLB VlbG. / Dornbirn, SKF / Steyr, Swarovski / Absam, Vorarlberger Kraftwerke / Bregenz, Wibeba / Vösendorf, Wilhelminenspital / Wien, Zumtobel / Dornbirn) haben ihre Kantinen und Getränke- sowie Verpflegungsautomaten auf die bargeldlose Zahlung mittels Quick umgestellt.
- Die Österreichische Mensen Betriebsgesellschaft mbH hat in allen Universitäten im Mensa-Bereich Quick-Zahlterminals installiert. Darüber hinaus wurden an der Johannes Kepler Universität in Linz alle Arten von Automaten mit Quick-Modulen ausgerüstet und die sog. Kepler-Card mit Quick-Chip als Studentenausweis ausgegeben. Die Universitäten in Salzburg und Innsbruck befinden sich in Vorbereitung.

## ***E-Commerce***

Ab sofort spielt Bezahlen mit Quick auch im E-Commerce eine Rolle. Mit @Quick ist es möglich, Waren und Dienstleistungen, welche im www angeboten werden, mittels Chipkarte online und ohne Risiko zu bezahlen. Voraussetzung für den Konsumenten ist neben einem Internet-Zugang eine Karte mit geladenem Quick-Chip und ein an den PC angeschlossenes Kartenlesegerät. Ein E-Commerce-Händler, der seinen Kunden ermöglichen will, über @Quick zu bezahlen, benötigt dafür weder eine eigene teure Hard- bzw. Softwarelösung, noch muss er über spezielles technisches Know-How verfügen. Über die gehostete Variante von @Quick ist es dem Händler möglich, dieses Service, ohne es selbst betreiben zu müssen, anzubieten. Der erste Shop, in dem mit der Elektronischen Geldbörse im Internet bereits bezahlt werden kann, ist unter <https://www.pdts.cc/shop/> zu finden. Hier kann man unter anderem auch die für @Quick notwendigen Kartenleser bestellen. Allgemeine Fragen, Anfragen zu den Konditionen und zum @Quick-Akzeptanzvertrag können per E-Mail an [martin.holzinger@europay.at](mailto:martin.holzinger@europay.at) gerichtet werden.

## ***Quick-Ladepromotion***

Von 1.4.2002 bis 30.6.2002 läuft eine Ladepromotion unter dem Motto ‚Jetzt Quick-Chip laden & gewinnen‘. Dabei bekommt jeder 1000ste Maestro-Karteninhaber, der seinen Quick-Chip auflädt, den geladenen Betrag (max. €400,-) zurückerstattet.

*Zum Autor:  
Produktmanagement Elektronische Geldbörse  
Europay Austria Zahlungsverkehrssysteme GmbH  
[Http://www.quick.at](http://www.quick.at), E-Mail: [quick@europay.at](mailto:quick@europay.at)*

*Prok. Robert Komatz, Europay Austria.*



# *Multifunktionaler Ausweis und Elektronische Signatur im Unternehmen*

## *1. Ausgangssituation*

In vielen Unternehmen sind mehrere verschiedene Schlüssel, Karten und Ausweise in Verwendung. Sie dienen meist zur Personenkontrolle (durch den Portier, ....), zur physikalischen Zutrittskontrolle zu Tresoren, Räumen, Gebäuden, Parkplätzen, Tiefgaragen etc., zur Abrechnung in der Kantine, zur innerbetrieblichen Zeitverrechnung, eventuell auch für den PC-Schutz etc.

Diese Situation ist für Unternehmen und ihre Mitarbeiter unbefriedigend, weil je Anwendungsgebiet unterschiedliche Produkte bereitgestellt, und für jeden einzelnen Mitarbeiter verwaltet und kontrolliert werden müssen. Vor allem die Verwaltung der verschiedenen Schlüssel und Karten, der erforderliche Aufwand, wenn ein Mitarbeiter einen oder mehrere dieser Schlüssel/Karten zu Hause vergisst, und der organisatorische, technische und finanzielle Aufwand nach einem Diebstahl bzw. Verlust eines Schlüssels/einer Karte, bereiten den Unternehmen unnötige Kosten und Zeitaufwendungen. Viele Unternehmen möchten daher die Zufahrts- / Zutrittskontrolle verbessern und vereinfachen, die interne Zeitkontrolle (Gleitzeitkontrolle, Stundenverrechnung etc.) auf eine moderne, administrativ einfache Form bringen, den Daten-, Geräte- und PC-Schutz effizienter gestalten, die Zahlungsfunktion im Betriebsrestaurant, bei Getränkeautomaten rationeller abwickeln etc. Die Unternehmen und Mitarbeiter wünschen sich auch eine Reduktion der Vielzahl an Schlüssel und Karten.

Die herkömmliche, handschriftliche Unterschrift spielt in Unternehmen eine sehr wichtige Rolle. Heute werden in Unternehmen praktisch alle Briefe, Angebote, Bestellungen, Verträge etc. auf Personalcomputer erstellt und zunehmend auch auf elektronische Weise versandt, vor allem durch den Einsatz von Internet und Intranets. Da in den meisten Unternehmen Digitale Signaturen noch nicht eingesetzt werden, führt das zunehmende Fehlen der Unterschrift zu einem bedeutenden Verlust an Sicherheit, an Vertrauenswürdigkeit und an Einhaltung der „Unternehmensregeln“ (insbesondere der Unterschriftenordnung). Viele Briefe, die nach der Unterschriftenordnung des Unternehmens bzw. den gesetzlichen Regelungen eine herkömmliche, handschriftliche Unterschrift erfordern, werden ohne Unterschrift versandt. Außerdem werden viele Briefe mit weniger vertraulichen Informationen, die früher durch den Briefumschlag einen ausreichenden Schutz hatten, per Internet ohne Verschlüsselung verschickt. Nur sehr vertrauliche Informationen werden meist geschützt. Weiters nehmen die externen Zugriffe auf wichtige Unternehmensdaten und der Datentransfer von sensiblen Daten über öffentliche Leitungen stark zu, es werden zunehmend wichtige Maschinen auch über größere

Entfernungen gesteuert und verwaltet, das Online-Angebot von Dienstleistungen mit sicherheitsrelevanten Daten nimmt zu etc. etc.

Der Einsatz der Digitalen Signatur und der Verschlüsselungstechnik wird daher immer wichtiger und sie entwickeln sich zu einem MUSS in allen Unternehmen.

## ***2. Multifunktionaler, chipkartenbasierender Unternehmensausweis***

Multifunktionale, chipkartenbasierende Unternehmensausweise (Unternehmenskarten) sind schon seit über 15 Jahren im Einsatz. In Österreich haben hier vor allem Geldinstitute wie die ERSTE Bank, Bank Austria und die PSK eine Pionierrolle gespielt.

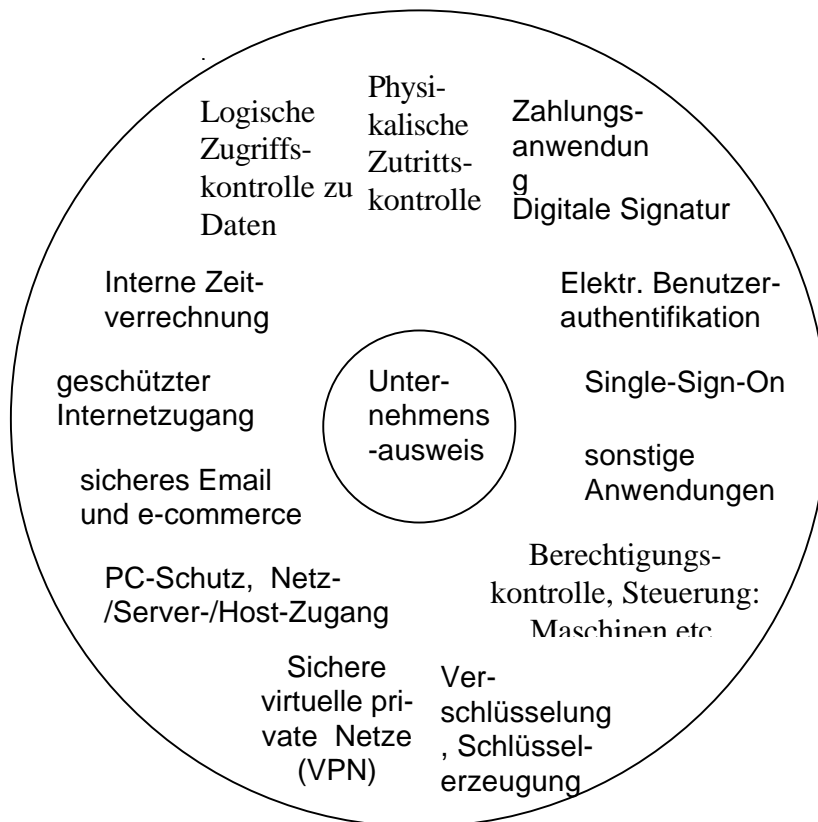
Begonnen hat es mit der herkömmlichen Personalausweisfunktion (mit Foto) und der Anwendung „physikalische Zutrittskontrolle“ zu Räumen, Gebäuden, Parkplätzen etc., zuerst mit kontaktbehafteten Karten, dann mit Kontaktloskarten. Es folgten Anwendungen wie z.B.:

- Elektronische Benutzerauthentifikation
- PC-Schutzsystem, Server-/Host-Zugangsschutzsystem (System-/Applikation-Logon, ...), logische Zugriffskontrolle zu Daten: diese Anwendungen machen es einem nicht Berechtigten unmöglich, Zugang zu einem PC, Server, Zentralrechner und den Anwendungen und Daten zu bekommen;
- Single-Sign-On: Es bietet dem berechtigten Anwender die Möglichkeit sich an einem einzigen Punkt des Systems einmal zu Beginn des Arbeitstages anzumelden und den seinem Profil entsprechenden Zugriff zu bekommen. Ein Vorteil ist auch die Senkung des Aufwandes für die Administration, die dadurch unabhängig von der Systemgröße zentral gehalten werden kann;
- Zahlungsfunktion: Getränkeautomat, Zigarettensautomat, Kantine (Zahlen, Essensbestellung, .....), Kopierer etc. Die Verwaltung von Zuschüssen (Essen-Bon etc.) für die Mitarbeiter;
- Berechtigungskontrolle für das „intelligente Gebäude“ (für die Einstellung / Parametrisierung diverser Steuerungen / Komponenten, für die automatische Anpassung an den Karteninhaber wie z.B. die gewünschte Raumtemperatur, für die Liftbenützung in bestimmte Stockwerke, ...), für Produktionsmaschinen (insbesondere externe Anlagen) etc.
- Innerbetriebliche Zeiterfassung: Gleitzeitkontrolle, Stundenverrechnung,...
- Datenverschlüsselung für kleine Datenmengen, Erzeugung bzw. Lieferung von Schlüsseln (z.B. Sessionkeys) für eine Datenverschlüsselung außerhalb der Karte: für die Echtzeitverschlüsselung größerer Datenmengen (z.B. die im Hintergrund in einem PC alle Daten auf der Festplatte stets verschlüsselt hält) sind kostengünstige Hardwarelösungen (z.B. in Form eines PCMCIA-Boards) am Markt verfügbar. Dadurch sind z.B. alle Daten eines gestohlenen Laptops absolut sicher geschützt.

In den letzten Jahren folgten durch den Einsatz von Public Key Infrastrukturen (PKI) weitere Anwendungen wie z.B.:

- Digitale Signatur für Dokumente jeder Art
- geschützter Internet-Zugang (Web-Logon, ...)
- sicheres Email
- sichere e-commerce und m-commerce Anwendungen
- sicheres VPN (virtuelles privates Netzwerk): es dient der Einrichtung von Intranets und Extranets und zum sicheren Fernzugriff von Daten
- Einbindung der oben angegebenen Anwendungen wie PC-Schutzsystem, Datenverschlüsselung, geschützter Server und Hostzugang und logische Zutrittskontrolle zu Daten in die Unternehmensausweis-basierende PKI

Durch das Laden mehrerer Anwendungen auf einen Unternehmensausweis und den Aufbau einer Unternehmensweiten PKI lassen sich umfangreiche Synergieeffekte und Sicherheitsverbesserungen erzielen.



Auf Bedarf können Chipkarten viele dieser Anwendungen so implementieren, dass der Karteninhaber bei der Anwendung anonym bleibt. Dies wird bei einigen Anwendungen entweder vom Unternehmen oder dem Karteninhaber gewünscht. Eine Anonymität gewährleisten können z.B. elektronische Geldbörsensysteme (für den Zahlungsverkehr in der Werkskantine, bei Automaten etc.) und elektronische Pseudonyme, die sich mit Chipkarten hervorragend realisieren lassen. Sie sollten überall dort eingesetzt werden, wo man

Datenspuren vermeiden möchte. Man kann mit einem chipkartenbasierenden Unternehmensausweis Lösungen mit direktem Personenbezug (Bezug zum Karteninhaber), mit Pseudonymität (Bezug auf ein Einzelindividuum innerhalb aller Karteninhaber eines Unternehmens, dessen Identität aber nicht erkennbar ist) und mit Anonymität implementieren.

Ziel vieler Unternehmen ist es, einen multifunktionalen, chipkartenbasierenden Unternehmensausweis für alle Mitarbeiter auszugeben, auf dem mehrere der oben angegebenen Anwendungen implementiert sind. Technologisch betrachtet können diese Karten ein Foto (Schwarzweiß oder Farbe), einen Text, einen „Kontaktlos-Chip“, einen „kontaktbehafteten Chip“, einen Barcode, einen Magnetstreifen und weitere Sicherheitsmerkmale enthalten. Die optische Gestaltung beinhaltet nicht nur das Corporate Design des Unternehmens, sondern z.B. auch Sicherheitsmerkmale, wie den laminierten Kartenkörper mit Guillochendruck – manipulationsgeschützt und durch ein glasklares „Overlay“ versiegelt. Der „Kontaktlos-Chip“ übernimmt in der Regel die Anwendungen physikalische Zutrittskontrolle und innerbetriebliche Zeitverrechnung, evt. auch eine Zahlungsfunktion, alle anderen Anwendungen übernimmt der „kontaktbehaftete Chip“.

Die neueste Anwendung, die die Unternehmensausweise revolutioniert, ist die PKI (Public Key Infrastructure). Sie verbessert nicht nur die Datensicherheit der internen und externen elektronischen Kommunikation und die Dokumentensicherheit, sondern ermöglicht vor allem auch eine Unterschrift. Die Unterschrift, die in Unternehmen eine sehr wichtige Rolle spielt, muss in Zukunft bei allen Unternehmen durch die stark zunehmende Bedeutung der elektronischen Kommunikation mit Hilfe der digitalen (elektronischen) Signatur erfolgen.

### ***3. Public Key Infrastructure (PKI)***

Eine Public Key Infrastructure (PKI) beseitigt die in den Unternehmen übliche Vielfalt an kryptografischen Datensicherungsverfahren. Es gibt nur noch eine vertrauenswürdige Netzwerkumgebung, in die sich die verschiedenen Anwendungen einbetten lassen. Alle Anwendungen nutzen eine einzige Sicherheitstechnologie, unabhängig davon, ob die Datenübertragung via Email, innerhalb einer e-/m-commerce Anwendung oder auf sonstiger Art und Weise innerhalb des Unternehmens oder nach außen gesichert und nachvollziehbar ablaufen soll, der Zugang zu Internet-Seiten, auf Dateien, PCs, Maschinen, Komponenten eines „intelligenten Gebäudes“ etc. durch Authentisierung geregelt oder ein Virtuelles Privates Netz (VPN) betrieben wird. Auch die meisten „alten“ Anwendungen der Unternehmensausweise (siehe oben Kap. 2) können auf Wunsch in die Unternehmensweite PKI eingebunden werden. Die Aufgabengebiete Digitale Signatur und Trust Center sind als notwendige Bestandteile einer PKI inhaltlich miteinander eng verknüpft. Kern der PKI ist der mit der Digitalen Signaturfunktion versehene Unternehmensausweis. Die PKI in einem Unternehmen kann als Zertifikatsinhaber neben den Unternehmensausweis-Inhabern auch nicht personenbezogene Objekte enthalten, wie z.B. eine Software, eine Anwendung, ein System, ein Unternehmen.

Die fünf wichtigsten Komponenten einer derartigen PKI sind dabei:

- die multifunktionalen Unternehmensausweise (siehe oben);
- die stationären und portablen Endgeräte mit integriertem oder externen Chipkartenleser. Hier reicht die Palette vom Desktop-PC, Laptop über PDAs (Personal Digital Assistants) hin bis zu Mobiltelefonen (z.B. Dual-Slot Handys), Komponenten eines „intelligenten Gebäudes“, Selbstbedienungsgeräten, Datenerfassungsgeräten, Produktionsmaschinen etc.
- geeignete „PKI-Software“. Hier ist vor allem eine sichere Software am Endgerät erforderlich;
- ein Trust Center (mit Zertifizierungsinstanz, Verzeichnisdienst, ....), das unter anderem die Zuordnung zwischen dem Unternehmensausweis und dem Ausweisinhaber herstellt;
- und die Registrierungsstelle, die für das richtige Erfassen der Unternehmensausweis-Inhaberdaten und die Übergabe der Unternehmensausweise an die richtige Person zuständig ist.

Ob die Digitale Signatur bei einem Unternehmensausweis eine „einfache“ sein kann oder eine „sichere“ (siehe Signaturgesetz / Signaturverordnung) sein muss und das Zertifikat ein qualifiziertes bzw. akkreditiertes (siehe Signaturgesetz / Signaturverordnung) sein muss, gehen die Expertenmeinungen auseinander. Beim Einsatz geeigneter, evaluierter Komponenten kann ein nicht-qualifiziertes Zertifikat gleich sicher sein wie ein qualifiziertes bzw. akkreditiertes Zertifikat. Ein Trust Center kann auch qualifizierte Zertifikate mit einfachen Signaturen ausgeben und es kann ein Trust Center auch nicht-qualifizierte Zertifikate mit sicheren Signaturen ausgeben, d.h. alle Variationen sind hier möglich.

Es ist in Unternehmen heute ein Trend zu erkennen, dass Unternehmensausweise mit digitaler Signaturfunktion und das Trust Center zwar die sicherheitstechnischen Voraussetzungen für eine gesetzeskonforme („sichere“) Signatur erfüllen sollen (z.B. Chipkarte mit ITSEC E3 hoch Evaluierung, sicheres Trust Center), dass sich aber die Unternehmen mit nicht-gesetzeskonformen Signaturen und Zertifikaten begnügen. Die Gründe dafür sind vor allem:

- In der internen Kommunikation und externen Kommunikation mit anderen Unternehmen besteht trotzdem die Rechtsgültigkeit der Signatur;
- Die Unternehmensausweise sind einfacher an die Mitarbeiter auszugeben und auch das Regelwerk bei Verlust, Diebstahl und Zerstörung kann einfacher sein;
- Die Zertifikate sind wesentlich kostengünstiger. Bei größeren Unternehmen wirkt sich der Preisunterschied ganz wesentlich aus;
- Die erforderliche Hardware (Chipkartenleser) und Software an den Endgeräten (wo signiert wird) ist wesentlich kostengünstiger und es kann praktisch alles signiert werden. Secure Viewer, wie sie bei „sicheren“ Signaturen benötigt werden, können nur wenige Datenformate signieren (z.B. XML-Dokumente). Dies bedeutet in der Praxis eine unakzeptable Einschränkung für Unternehmen;
- Es existiert ein ausreichendes Angebot an geeigneten, sicheren Trust Centers;
- Die Multifunktionalität der Unternehmensausweise ist problemlos realisierbar. Bei „sicheren“ Signaturen kommt man auch hier zu praktisch unakzeptablen Einschränkungen für Unternehmen.

Trotzdem benötigen in Zukunft Unternehmen auch Chipkarten für „sichere“ Signaturen. Diese werden vor allem für die elektronische Kommunikation mit öffentlichen Stellen benötigt. Die Anzahl dieser „speziellen“ Chipkarten kann aber verhältnismäßig klein gehalten werden in Relation zu den multifunktionalen Unternehmensausweisen mit Digitaler Signatur. Daher spielen bei diesen Spezialkarten die kompliziertere Ausgabe, die eingeschränkte Multifunktionalität und der höhere Preis der Zertifikate keine bedeutende Rolle.

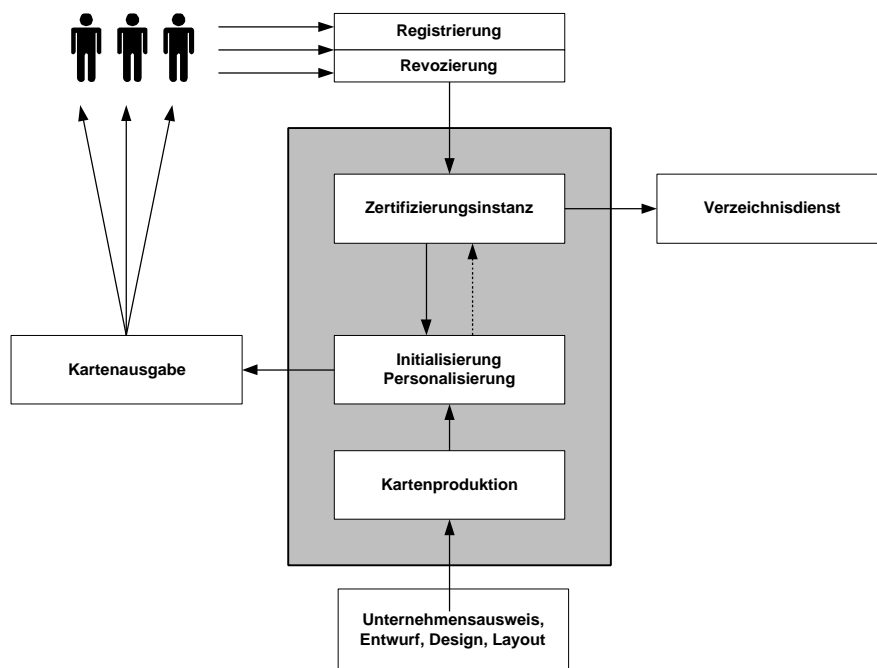
Die Digitale Signatur hat den wesentlichen Vorteil, dass eine feste Zuordnung zwischen Dokument und Unterschrift und Person besteht. Das heißt, dass die Digitale Signatur garantiert, dass das Dokument nachträglich nicht verändert wurde, die Unterschrift genau zum vorliegenden Dokument gehört und die unterzeichnete Person zum Dokument und zur Unterschrift gehört. Bei der herkömmlichen eigenhändigen Unterschrift kann der Empfänger eines Dokumentes Veränderungen am Dokument nicht erkennen (z.B. wenn bei einem 20 Seiten langen Vertrag die 12. Seite ausgetauscht wurde, Paraphierungen stellen hier nur eine kleine Verbesserung dar). Er kann in der Regel auch nicht erkennen, ob die Unterschrift echt ist, das heißt zur unterzeichneten Person gehört. Dazu müsste er die Unterschrift sehr genau kennen (was meist nicht der Fall ist) oder er müsste eine Unterschriftenvorlage besitzen (was bei Banken der Fall ist, im Wirtschaftsleben aber sehr selten ist). Ebenso ist die Einhaltung und Kontrolle der Unterschriftenordnung eines Unternehmens leichter zu garantieren. Es ist sogar möglich, mit einigen Einschränkungen eine automatische Überprüfung der Unterschriftenordnung für alle elektronischen Dokumente durchzuführen.

Außerdem kann sich der Karteninhaber mit seinem Unternehmensausweis und der Digitalen Signatur gegenüber jeder Anwendung, jedem System, jedem anderen Unternehmen bzw. Person identifizieren, um gewisse Aktivitäten zu veranlassen, um gewünschte Leistungen zu erhalten, Zugriff zu gewissen Daten zu erhalten, bestimmte Software zu aktivieren etc.

Der Einsatz der Digitalen Signatur besitzt für Unternehmen also eine Menge von wesentlichen Sicherheitsvorteilen und Rationalisierungsmöglichkeiten bei der internen und externen Kommunikation, der Daten-/Dokumenten-Bearbeitung, der Daten-/Dokumenten-Ablage etc.

#### ***4. Digitale Signatur im Unternehmen***

Mit digitalen Signaturen kann der gesamte elektronische Datenverkehr – unabhängig vom Übertragungsmedium – nachweislich abgesichert werden, und das nicht nur innerbetrieblich, sondern auch nach außen mit Geschäftspartnern und Kunden. Auch Archivierungen, an denen nachträgliche Änderungen erkennbar sein müssen, sind mit digitalen Signaturen durchführbar. Die Verwendung digitaler Signaturen durch die Mitarbeiter eines Unternehmens erfordert eine sogenannte Public Key Infrastruktur (PKI), in welcher der gesamte Lebenszyklus digitaler Signaturen abgebildet ist. Dieser Lebenszyklus umfasst die Registrierung der Benutzer, die Erstellung der Zertifikate mit anschließender Eintragung in ein öffentlich zugängliches Verzeichnis, die Herstellung, Initialisierung und Personalisierung der Unternehmenskarten, die Ausgabe der Unternehmenskarten und der zugehörigen Passwörter an den Benutzer sowie die Suspendierung und Revozierung der Zertifikate.



Die Mitarbeiter des Unternehmens und die sonstigen Personen, die Anspruch auf einen Unternehmensausweis mit Digitaler Signatur haben, müssen eine der Registrierungsstellen (z.B. das Personalbüro) besuchen, um ihre „Digitale Signaturfunktion“ zu beantragen. Die Registrierung erfolgt in der Regel direkt beim Unternehmen. Die Anträge können vom Unternehmen auch gesammelt aus einer eventuell vorhandenen Personaldatenbank generiert werden.

Die Registrierungsanfragen gelangen zur Zertifizierungsinstanz des Trust Centers, dem zentralen Bestandteil einer PKI. Dort findet die nachweisliche Zuordnung eines öffentlichen Schlüssels zu einem Benutzer statt. Die Schlüsselgenerierung selbst kann an mehreren Orten stattfinden und ist abhängig vom zuvor festgelegten Sicherheitsniveau. Die Schlüsselgenerierung für die Digitale Signatur erfolgt nur im Unternehmensausweis, der geheime Schlüssel ist vom Unternehmensausweis nicht auslesbar. Dieser Vorgang ist ein Teil der Initialisierungsphase im Anschluss an die Kartenproduktion. Bei der Initialisierung werden im Chip unter anderem auch alle Dateien inklusive Zugriffsrechte angelegt. Die Festlegung der Dateihierarchien, Dateien, Zugriffsrechte, Datenstrukturen etc. muss genau geplant werden, da hier Fehler bzw. eine Nichtberücksichtigung von zukünftigen Anwendungen nachträglich große Probleme bzw. Aufwendungen verursachen können. Zum Beispiel muss hier auch festgelegt werden, wie viele Zertifikate (z.B. ein „SSL-Zertifikat“, ein „S/MIME Zertifikat“ und ein Root-Zertifikat) und wie viele Schlüsselpaare für die Digitale Signatur angelegt werden und welche und wie viele Schlüssel für Verschlüsselungen (symmetrisch / asymmetrisch) benötigt werden.

Der Initialisierung folgt die Kartenpersonalisierung, die beim Kartenhersteller, aber auf Bedarf auch direkt im Unternehmen stattfinden kann. Basierend auf den Anforderungen des Unternehmens und der dort verwendeten Software und Hardware wird eine rasche Personalisierung der benötigten Unternehmensausweise möglich. Die Personalisierung der Erstausrüstung erfolgt in der Regel beim Kartenhersteller, für die weiteren

Unternehmensausweise für neue Mitarbeiter, verlorene Ausweise, Unternehmensausweise für Besucher, Wartungstechniker etc. erfolgt in der Regel beim Unternehmen selbst. Auch die Personalisierung muss genau geplant werden, damit das Unternehmen an zukünftige Anforderungen rasch und kostengünstig reagieren kann.

Die Initialisierungs- und Personalisierungsprozesse sind für Unternehmensausweise mit Digitaler Signaturfunktion etwas komplexer, da zusätzlich zu den üblichen Tätigkeiten unter anderem auch die Erzeugung des Schlüsselpaares vom Chip selbst, die Weitergabe des öffentlichen Schlüssels vom Chip zum Trust Center (zur Zertifizierungsinstanz) inklusive weiterer Daten für die Zertifikatserstellung und die Übertragung des Zertifikats vom Trust Center zum Unternehmensausweis notwendig sind.

Neben der rein kartenorientierten Betrachtung, muss natürlich auch die erforderliche Organisation, Software und Hardware genau geplant werden, ein geeignetes Sicherheitskonzept vorliegen etc. In diesen Bereichen sind vor der Einführung des multifunktionalen Unternehmensausweises umfangreiche Aufgaben zu erledigen.

Das Angebot an geeigneten Trust Centers ist in Europa derzeit schon ausreichend gut. Große Unternehmen versuchen oftmals trotzdem, ein eigenes Trust Center aufzubauen. Ob sich dieses Vorhaben rechnet, kann bezweifelt werden. Außerdem bieten viele Trust Centers auch ein Hosting an, das heißt Unternehmen können ihr Trust Center einfach und kostengünstig „outsourcen“.

Multifunktionale, chipkartenbasierende Unternehmensausweise wurden schon in den achtziger Jahren in vielen Unternehmen erfolgreich eingeführt. Die Integration der Digitalen Signatur ist aber noch neu. In Deutschland haben z.B. die Autounternehmen BMW und Audi derartige Karten eingeführt. Bei BMW wurden schon rund 160.000 multifunktionale Unternehmensausweise an allen Mitarbeiter ausgegeben, davon haben rund 60.000 Karten auch die Digitale Signaturfunktion.

## ***5. Zusammenfassung***

Der große Bedarf am Einsatz von multifunktionalen, chipkartenbasierenden Unternehmensausweisen, von diversen chipkartenbasierenden Sicherheitsprodukten für den PC-Schutz, Datenschutz, die Datenverschlüsselung etc. sowie von digitalen Signaturen in Unternehmen steht außer Zweifel. Die Sicherheitsverbesserungen und Rationalisierungseffekte sind bekannt. Einige Unternehmen haben den Schritt zur multifunktionalen Unternehmenskarte mit Digitaler Signaturfunktion schon gemacht, wenn auch teilweise noch etwas zaghaft. In der Zukunft werden sicher viele Unternehmen diesen Schritt mehr oder weniger umfangreich tun und es nicht bereuen. Voraussetzung ist aber eine gute Planung, Produktauswahl und Implementierung.

Weitere Informationen zu diesem Thema erhalten Sie vom Autor unter [ernst.piller@winter-ag.com](mailto:ernst.piller@winter-ag.com)

*Autor:*

*Dr. Ernst Piller*

*Vorstand der Winter AG*



# **Eine Dual-Interface** **SmartCard mit schaltbarer** **kontaktloser** **Datenübertragung** **zur Serviceabrechnung von** **Verkehrsdienstleistungen**

## ***Überblick***

Die Anwendungsfelder einer Chipkarte mit schaltbarer kontaktloser Übertragung im Bereich der Serviceverrechnung (,Ticketing') werden beleuchtet, wobei vor allem die Anwendung als elektronisches Ticket zur Abrechnung von Verkehrsdienstleistungen von Interesse ist.

Dabei wird die gedruckte Antenne einer Chipkarte mit kontaktlosem Interface durch einen Taster eingeschaltet, und somit wird die kontaktlose Datenübertragung durch eine bewusste Handlung des Kartenbenutzers aktiviert.

Der vorliegende Artikel beschreibt die von der Fa. Austria Card patentierte Produktinnovation einer schaltbaren ,kontaktlosen Chipkarte mit Transponderspule'.

Weiters wird ein gefördertes Forschungsprojekt der Firma Austria Card vorgestellt, das eine kombinierte Zahlungsverkehrskarte mit kontaktbehalteter Datenübertragung und einer Ticketing-Anwendung deren Werteinheiten über ein kontaktloses Interface abgebucht werden können, als marktreifes Produkt zum Ziel hat. Zentrales Bauelement einer solchen Karte ist ein Dual-Interface-Chip.

## ***Dual-Interface Chipkarten***

Bereits seit mehreren Jahren sind Dual-Interface-SmartCard-ICs erhältlich.

Diese IC-Typen sind Microcontroller mit einer Basis-CPU, z.B. einem 8051-Prozessor und verschiedenen weiteren integrierten Funktionsmodulen, wie ROM-, RAM- und EEPROM-Speicher, serieller Schnittstelle sowie kryptografischem Coprozessor. Der wesentliche Unterschied zu Chips für kontaktbehaltete Karten ist bei Dual-Interface-SmartCard-ICs die zweifache Ausführung der seriellen Schnittstelle als kontaktbehaltete Schnittstelle nach ISO7816 und als kontaktlose Schnittstelle nach ISO14443 (Proximity Coupling, also Übertragung im mittleren Entfernungsbereich zum Kartenleser).

Der Implantierungsprozess des Chips, der Kontaktflächen und der Antenne für die kontaktlose Übertragung auf einer Plastikkarte erfordert in der Produktion eine Anpassung von Maschinen und Steuerungssoftware gegenüber der Implantierung von Chips mit rein kontaktbehafteter oder rein kontaktloser Schnittstelle.

## ***Das Patent der schaltbaren ‚kontaktlosen Chipkarte mit Transponderspule‘***

Das Patent EP 0 946 926 ‚Kontaktlose Chipkarte mit Transponderspule‘ der Fa. Austria Card [1] (Erfinder: M. Prancz) betrifft eine schaltbare kontaktlose Chipkarte mit Transponderspule und ein Verfahren zu deren Herstellung.

Gegenstand des Patents ist eine Identifikationskarte mit Transponderspule und eingebautem Chipmodul, wobei die auf dem Chipmodul gespeicherten Daten ausgelesen und mit Hilfe der Transponderspule kontaktlos auf ein Lesegerät übertragen werden.

Identifikationskarten zur kontaktlosen Transaktion werden für die unterschiedlichsten Anwendungen einer Standardisierung unterworfen. Zielsetzung aller dieser Normen ist die Erhöhung der Sicherheit und der Geschwindigkeit von Identifikations- und Transaktionsvorgänge bei gleichzeitiger Reduktion der integralen Kosten und einer weltweiten Anwendung und Kompatibilität.

Identifikationsvorgänge mittels berührungsloser Identifikationskarten werden in immer stärkerem Ausmaß im öffentlichen Personen- und Nahverkehr bzw. ganz allgemein zur komfortablen und raschen Identifikation bzw. Zutrittskontrolle und oftmals der vollautomatischen Abbuchung entsprechender Werteinheiten oder Geldbeträge verwendet.

Im überwiegenden Maße wird diese rasche und unbemerkte Identifikation sinnvoll und vom Besitzer voll akzeptiert stattfinden.

Ein missbräuchlicher Zugriff auf eine solche Karte – z.B. das automatische Auslesen von personenbezogenen Daten über ein Lesegerät - ist für den Kartenbenutzer erst rückwirkend festzustellen. Aus diesem Grund werden Geldtransaktionen ausschließlich mittels kontaktbehafteter Chipkarten durchgeführt und der Transaktionsvorgang bewusst und oftmals nur nach Eingabe einer persönlichen Identifikationsnummer (PIN) durchgeführt.

Bei allen Arten von Identifikationskarten-Applikationen mittels berührungsloser Transponder-Chipkarten müssen die Aspekte der länderweit durchaus sehr unterschiedlichen Datenschutzgesetze und Verordnungen bzw. ganz allgemein der guten Sitte berücksichtigt werden.

Die Innovation, die durch das Patent geschützt wird, ist, eine Chipkarte der eingangs erwähnten Art so weiterzuentwickeln, dass mittels eines kostengünstigen Prozesses ein einfach anwendbares Produkt dem Benutzer einer derartigen berührungslos funktionierenden Chipkarte die Möglichkeit gibt, den Vorgang der Identifikation und Transaktion bewusst herbeizuführen und damit im rechtlichen Rahmen nationaler Datenschutzgesetzen zu bleiben.

Wesentlich bei der vorliegenden Erfindung ist die bewusste Schaltung der Transponderspule, wobei bevorzugt die Kontaktfläche der Transponderspule und die zugeordneten Kontaktflächen eines Tasters durch die willkürliche Schaltung miteinander verbunden werden.

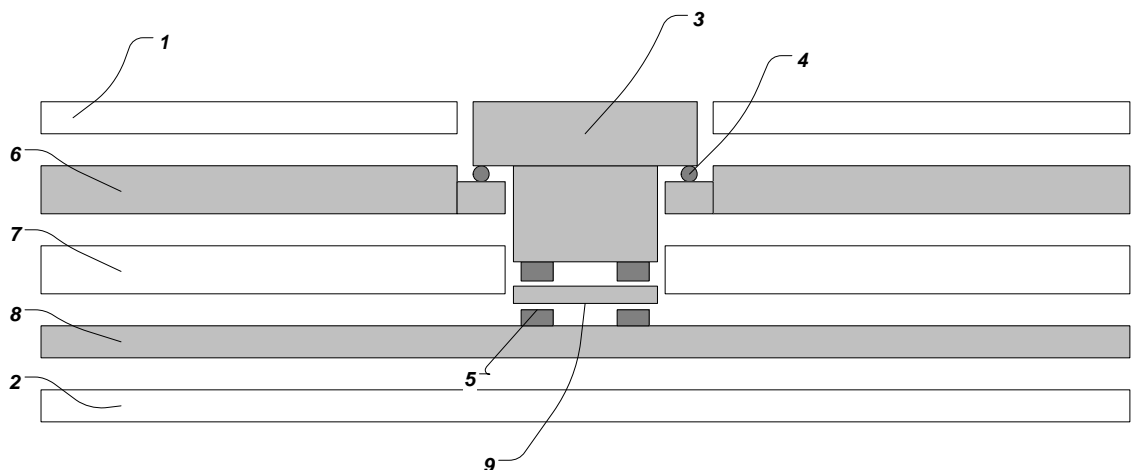


Abbildung 1: Schematischer Querschnitt durch die Karte

Abbildung 1 gibt den Querschnitt durch die Karte wie sie in [1] dargestellt ist vereinfacht wieder. Dabei sind 1 und 2 Deckfolien, 6-8 innere Folien, wobei 7 als Kernfolie bezeichnet wird.

Die eigentliche Funktionalität des Schaltens wird durch 3-5 erfüllt, wobei 3 das bewegte Schalterelement ist, 4 ist eine elastische Klebeschicht und 5 sind die Kontaktflächen. Zwischen den Kontaktflächen befindet sich ein weiteres Schaltelement 9, das aus einem Material gefertigt ist, das erst bei Druck leitfähig wird und die Kontaktflächen elektrisch verbindet.

## ***Anwendungen bei der Serviceverrechnung von Verkehrsdienstleistungen***

Es gibt in der Fachliteratur unterschiedliche Verwendung des Begriffs Ticketing. Hier wird er zunächst in dem Sinn verwendet, dass jedes Service, das durch Einlösen einer Berechtigung (eines Tickets) in Anspruch genommen werden kann, zum Anwendungsbereich des Ticketings gehört. Durch die Karte weist der Karteninhaber die Berechtigung nach, das Service zu beanspruchen. Der Wert der eingelösten Karte wird durch einen Zahlungsvorgang des Nutznießers des Services abgegolten entweder vor (z.B. Skilift) oder nach (z.B. Parkhaus) der Inanspruchnahme des Services. Die Karte kann dabei als materielles Gut vorliegen (Papierticket, Pre-Paid-Karte) und nur einmal verwendbar sein oder auf einen materiellen Träger in immaterieller Form (als Information) geladen werden – dann ist der materielle Träger (z.B. eine Chipkarte) mehrmals für die Benutzung ein und desselben oder verschiedener Services verwendbar. Die ladbare Berechtigung kann wiederum eine von mehreren Anwendungen auf einer Smart Card sein – im vorliegenden Fall also eine weitere Anwendung neben einer Zahlungsverkehrsanwendung.

Als Anwendungsgebiet des Ticketing sind die verschiedensten Services denkbar: Veranstaltungen wie Konzerte und Sportveranstaltungen und vor allem die Benützung von Verkehrsdienstleistungen auf Skiliften, in Parkhäusern, der Eisenbahn, der Verkehrsmittel des öffentlichen Personen und Nahverkehrs (ÖPNV), von Car-Sharing-Unternehmen sowie von

Fluglinien. Auch die Benützung der Straßen durch den Güter- oder Personenverkehr ist eine Leistung, deren Abgeltung zur Diskussion steht.

## ***Internationale Lösungen***

Wesentliche Entwicklungen im Bereich des Ticketing für Verkehrsdienstleistungen und vor allem des ÖPNV – der elektronische Fahrkarte - finden in Europa in Deutschland, Frankreich und Großbritannien statt, Feldversuche und umgesetzte Lösungen sind auch in anderen Ländern zu finden.

Weltweit findet man Lösungen sowohl im amerikanischen wie auch im asiatischen Raum.

Auch vom Internationalen Verband für öffentliches Verkehrswesen (UITP - Union Internationale des Transportes Public) werden Stellungnahmen zum Thema veröffentlicht.

## ***Beispiel Österreich***

In Bussen des Oberösterreichischen Verkehrsverbundes in Steyr und Wels ein Ticketing-System für Busse realisiert. Der Fahrgast hat eine Chipkarte, die im Fahrzeug registriert wird und den Bestpreis garantiert. Die Karte kann beim Fahrer oder an Automaten mit einem zusätzlichen Guthaben aufgeladen werden.

## ***Zusammenfassung und weiteres Vorgehen***

Es wurde auf Basis einer konzeptionellen patentierten Produktinnovation der Fa. Austria Card die Anwendungsmöglichkeit im Bereich der Serviceabrechnung von Verkehrsdienstleistungen dargestellt.

Weiter Schritte sind die Realisierung des patentierten Konzepts in einem Gebrauchsmuster und die Überführung in ein marktreifes Produkt.

Die Produktion einer Testserie von Karten mit Dual-Interface Chip und kombinierter Zahlungsverkehr und Ticketing-Anwendung erfolgt im Rahmen eines geförderten Forschungsprojekts [2].

Die Zulassung durch Austrian Payment Systems Services (APSS) und der Einsatz bei nationalen und internationalen Pilotversuchen im Bereich der Serviceabrechnung von Verkehrsdienstleistungen werden angestrebt.

### *Literatur*

[1] Austria Card GmbH, Europäische Patentschrift, Kontaktlose Chipkarte mit Transponderspule, EP 0 946 926 B1, Patenblatt 2001/50, 12.12.2001

[2] Knezu C., Manninger M., BAkeT – Bankkarte mit kontaktlosem elektronischen Ticketing, Forschungsantrag an den Kompetenzzentrumfond der OeNB, 9.01.2002

### *Danksagung*

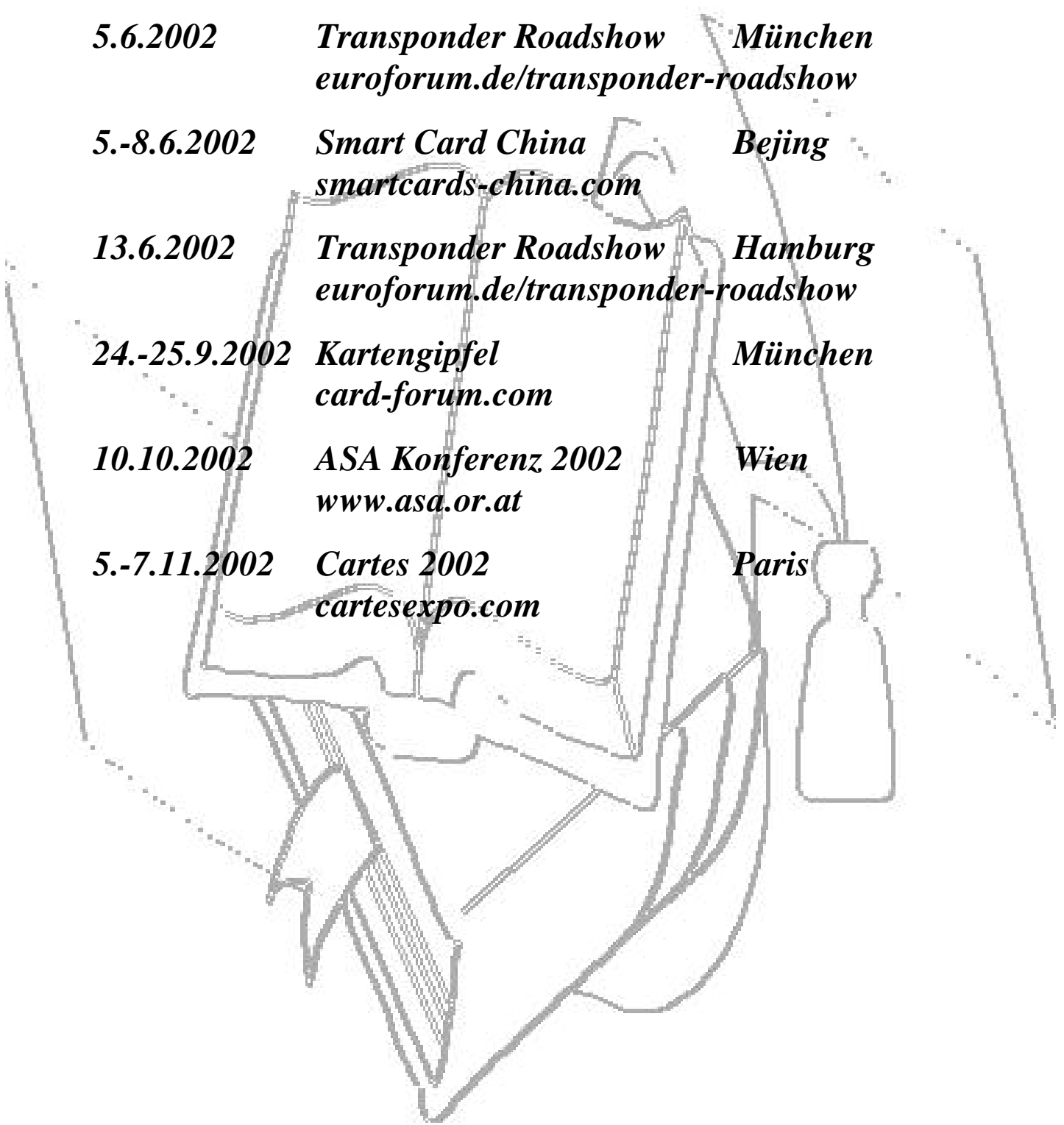
Die Autoren danken Mag. Dipl.-Ing. Dr. techn. Martin Manninger für zahlreiche Anregungen.

### *Autoren*

Dipl.-Ing. Dr. techn. Clemens Knezu, clemens.knezu@austriacard.at und Ing. Erik Mitterhofer, beide Austria Card GmbH A-1232 Wien, Lamezanstraße 4-8 ◆

# Veranstaltungen

*Konferenzen, Messen*

- 
- |                      |   |                |
|----------------------|---|----------------|
| <b>5.6.2002</b>      | <b>Transponder Roadshow</b><br><i>euroforum.de/transponder-roadshow</i> | <b>München</b> |
| <b>5.-8.6.2002</b>   | <b>Smart Card China</b><br><i>smartcards-china.com</i>                  | <b>Bejing</b>  |
| <b>13.6.2002</b>     | <b>Transponder Roadshow</b><br><i>euroforum.de/transponder-roadshow</i> | <b>Hamburg</b> |
| <b>24.-25.9.2002</b> | <b>Kartengipfel</b><br><i>card-forum.com</i>                            | <b>München</b> |
| <b>10.10.2002</b>    | <b>ASA Konferenz 2002</b><br><i>www.asa.or.at</i>                       | <b>Wien</b>    |
| <b>5.-7.11.2002</b>  | <b>Cartes 2002</b><br><i>cartesexpo.com</i>                             | <b>Paris</b>   |

# **ASA Konferenz 2002**

## ***Kontaktlose Chipkarten***

### ***Normierung - Produkte - Anwendungen***

Bewährte Standards – ISO14443, ISO15693, .. – , Produktinnovationen und zügig voranschreitende Standardisierungsarbeit bringen Schwung in den Markt der Kontaktlosanwendungen. Komponentenhersteller und Systemintegratoren bieten heute schon eine Vielfalt an attraktiven und kundenfreundlichen Lösungen für ihre Kunden.

Positive Markterwartungen, interessante Applikationen und viele neue Technologien am Sektor RFID werden das Thema „Kontaktlose Chipkarten“ auf der ASA Konferenz 2002 begleiten.

**10. Oktober 2002**, von 9.00 bis 17.00 Uhr,  
Hotel Renaissance,  
Linke Wienzeile / Ullmannstraße 71,  
1150 Wien (U-Bahnstation Meidlinger Hauptstraße)

### **Themenauszug**

- Normierung
- ÖPNV
- Logistik, Supply Chain Management
- Zahlungsverkehr, Dual Interface
- Multifunktionale Unternehmenskarte
- Tourismus

Das genaue Tagungsprogramm finden Sie ab Mitte August auf unserer Homepage <http://www.asa.or.at>

### **Mitgliedschaft Jahresbeitrag**

persönliches Mitglied	Euro 14,--
Firmenmitglied	Euro 65,--
förderndes Mitglied	Euro 218,--

### **Konferenzgebühr**

ASA Mitglied	Euro 200,--
nicht ASA Mitglied	Euro 276,--



**Recht erholsame Urlaubstage wünscht Ihnen die  
Austrian Smart – Card Association**