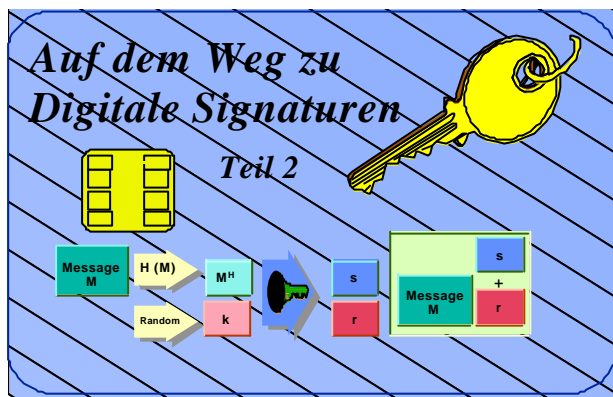


ASA NEWS

Digitale Signaturen



Nachdem im ersten Teil die allgemeinen Grundlagen der Digitalen Signatur beleuchtet wurden, soll hier ihr konkretes Anwendungsszenario aus Sicht der österreichischen Kreditwirtschaft dargestellt werden. An erster Stelle stehen hier die Anwendungen aus dem elektronischen Zahlungsverkehr, welche den Mittelpunkt des Begriffs "Electronic Banking" darstellen.

Motivationen und Prämissen im elektronischen Zahlungsverkehr

Da die konventionellen Methoden (Bargeld, Zahlschein, Erlagschein, Schecks, u.s.w) sowohl aus betriebs- wie volkswirtschaftlicher Sicht erheblichen Kosten- wie Zeitaufwand verursachen, haben die Kreditinstitute schon vor Jahren elektronische Ersatzverfahren entwickelt und ausgebaut. Die bekanntesten sind einerseits die bargeldlosen Zahlungen mit Hilfe von Plastikkarten, andererseits Zahlungen und Kontoauszüge vom / zum PC über Datenleitungen bzw. Datenträgern (Electronic Banking).

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

internet: http://www.asa.or.at

Nr. 10 September 1998

Inhalt

Digitale Signaturen 1

Motivationen und Prämissen im elektronischen Zahlungsverkehr 1

Infrastrukturprojekt "Elektronische Unterschrift" der Banken 4

Die wichtigsten Funktionen 6

Designkriterien 7

Stand der rechtlichen Rahmenbedingungen 9

Absehbare Perspektiven 11

Quick im Internet 13

Quick Classic 13

Auftritt Internet 13

Zahlen übers Internet 14

Quick im Internet : Die drei Teile 15

So funktioniert's: 16

Mit Korrektur 17

Kartenleser - jetzt und zukünftig 17

Echteinsatz und Zukunft 17

Veranstaltungen 19

Konferenzen, Messen 19

Deutschland - Österreich - Schweiz: Kartengipfel '98 20

ASA Jahrestagung 1998 "Digitale Signatur" 23

Zur Zeit wird bereits rund die Hälfte aller geschäftlichen Zahlungen papierlos abgewickelt. Dieser Trend wird anhalten und sich weiter verstärken.

Während bei den Plastikkarten der Besitz der Karte bereits ein Mittel zur Autorisierung der Zahlung darstellt, müssen beim Electronic Banking manuelle Hilfsmittel verwendet werden, wie das PIN/TAN Verfahren oder der Datenträger-Begleitzettel. Sie erfordern eine aufwendige Logistik sowohl bei der Bank wie beim Kunden und stellen hohe Ansprüche an den sicheren Umgang damit. Wer auch immer im Besitz einer gültigen TAN (Transaktionsnummer) ist, kann damit die zugehörige Zahlung auslösen. Dies unter Anbetracht von erheblichen Werten (etwa einer kompletten Gehaltsüberweisung eines Betriebes) sowie sensiblen Transaktionen wie Einzugsaufträgen. Da vor allem das System des Benutzers der Virengefahr ausgesetzt ist, müssen die Maßnahmen zu ihrer Abwehr ständig ausgebaut werden. Ob das PIN-/TAN Verfahren für den Benutzer als einfach oder aufwendig empfunden wird, hängt von seinen Gegebenheiten ab: Hat er nur ein Konto, dann ist es für ihn kein besonderes Problem, die jeweils richtige TAN anzuwenden. Handelt es sich etwa um eine größere Firma mit mehreren auch internationalen Bankverbindungen und ist die Zeichnung seitens mehrerer Personen erforderlich, dann sind auch mehrere TAN-Listen oder gar unterschiedliche Verfahren im Spiel. Bei Fehlgriffen sind dann Rücksprachen erforderlich, welche auch für die Banken aufwendig sind.

Somit ergab sich zunächst im kommerziellen Anwendungsbereich des Electronic Banking der Bedarf nach einem automatisierbaren Verfahren, Zahlungen authentisch und gleichzeitig auch einen sicherheitstechnischen Technologiesprung zu machen. Dabei erwies sich bald die Digitale Signatur als einzig zukunftsweisende Lösung für sichere Zahlung als grundlegende Bankdienstleistung.

Mit der Wahl des zukünftigen Verfahrens gingen die **grundsätzlichen Anforderungen** der Banken einher:

- **Sicherheit:** Primär sind die Institute Anwender von Technologie und Infrastruktur. Umgesetzt auf Digitale Signaturen sind sie diejenigen, welche sie verifizieren und schließlich Geld bewegen müssen. Somit ist klar, daß sie dafür einen vernünftigen und angemessenen Sicherheitsstandard fordern. Ein solcher muß vor allem berücksichtigen, daß elektronischer Betrug weit gefährlicher werden kann als die Fälschung von Bargeld, da elektronische Daten schneller und weiträumiger verbreitet werden können. Geht man davon aus, daß es in keinem von Menschen errichteten System 100% Sicherheit gibt, muß die absolute Forderung lauten, daß sich Attacken auf elektronische Zahlungssysteme niemals lohnen dürfen. Das heißt, der Aufwand für einen Betrug muß weit höher sein als der erzielbare Nutzen für den Angreifer. Damit ist - von irrationalen Einzelfällen abgesehen - die wesentlichste Motivation, nämlich die betrügerische Bereicherung genommen.
- **Interoperabilität:** Zahlungen werden nicht zum Selbstzweck geleistet, sondern sind immer mit Grundgeschäften verbunden. Dies ist bei allen spezialisierten Zahlungssystemen wie etwa den Kartensystemen durchgängig; in einem Arbeitsgang liefert eine Registrierkasse die Daten für die Buchhaltung, Warenwirtschaft und die Zahlung. Für das Electronic Banking, welches mehr oder weniger den konventionellen Vorgang abbildet, ermöglichen Medien wie das Internet ebenso integrierte Abläufe - in einem Zug kann elektronisch bestellt und bezahlt werden; mit der Digitalen Signatur als Willenserklärung. Der Benutzer würde es kaum verstehen, daß er dafür pro Anwendung unterschiedliche Verfahren bzw. Hilfsmittel einsetzen müßte. Er wird also um so mehr motiviert sein sich die notwendigen Einrichtungen wie z.B. einen Chipkartenleser zu beschaffen, je größer die Palette an Einsatzgebieten ist, die er vorfindet. Somit kann ein System für Digitale

Signaturen nur dann erfolgreich sein, wenn es für alle passenden Anwendungen zur Verfügung steht. In der Praxis bedeutet dies allerdings, rechtzeitig für die wechselseitige technische Kompatibilität und rechtlich einwandfreie Anerkennung der Digitalen Signaturen und Zertifikate durch die Geschäftspartner zu sorgen. Dies ist keineswegs einfach, wenn man die globalen Dimensionen des elektronischen Geschäftsverkehrs berücksichtigt. Jede Organisation, die Digitale Signaturen anwenden will, muß einerseits schnell und umfassend konkrete Systeme entwickeln, andererseits auf die Einhaltung von Normen und Standards achten, welche gerade in der rasant entwickelnden Kommunikationstechnologie viele Optionen und damit mögliche Inkompatibilitäten bietet.

- **Convenience:** Digitale Signaturen erfordern komplexe Technologien und Infrastrukturen. Davon soll der Benutzer aber möglichst nicht berührt werden. Einfach, sicher und schnell soll alles gehen, dann bringt es ihm einen Nutzen im Vergleich zur manuellen Unterschrift, denn diese ist für ihn kaum aufwendig.
- **Standortfaktor:** Auch die österreichische Kreditwirtschaft ist von der zunehmenden internationalen Verflechtung betroffen und kann sich der oft zitierten Globalisierung nicht entziehen. Die Senkung von unproduktiven Kosten stellt für sie eine der wichtigsten Voraussetzungen dar, um im internationalen Wettbewerb bestehen zu können. Kapazitäten, welche für die Bearbeitung von Zahlungsaufträgen gebunden sind, müssen in immer stärkerem Ausmaß für Beratung und Service immer anspruchsvoller werdender Kunden verfügbar gemacht werden, wobei die Ertragspotentiale keineswegs im gleichen Ausmaß mitwachsen.

Für ein kleines europäisches Land liegen die guten Chancen dort, wo man individuelle und maßgeschneiderte Dienste anbieten kann. Deren technische Abbildung erfordert vor allem Kompetenz und Flexibilität. So ist es in einigen wichtigen Bereichen nicht zielführend, bereits im großen Stil angebotene Lösungen nachzuahmen, selbst wenn dies im ersten Moment als billigste Variante erscheint. Bei Systementscheidungen bedeutet das, ob man die fertige Lösung importieren oder eigene auch technische Kompetenz aufbauen soll, mit der man sich dann qualitativ von den Mitbewerbern unterscheidet. Da dies der aufwendigere Weg ist, gilt es sämtliche innovativen Potentiale in Österreich bzw. Europa sinnvoll zu nutzen und auszubauen. Günstig ist hier das traditionell kooperative Klima, um das uns viele Länder beneiden.

Infrastrukturprojekt "Elektronische Unterschrift" der Banken

Projektverlauf

Aus der nun dargestellten Motivation entstand zunächst eine Machbarkeitsstudie für den Einsatz der Digitalen Signaturen im Bankbereich. Diese wurde von der gemeinsamen Tochterfirma STUZZA (Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr) auf Basis der genannten Prämissen sowie der bereits vorhandenen Möglichkeiten im Jahr 1996 unter dem Projekttitel "Elektronische Unterschrift" erarbeitet. Sie mündete in die Empfehlung, daß die österreichischen Banken in ihrem Bereich eine eigene, aber anderen Anwendungen gegenüber offene Infrastruktur errichten und

betreiben sollten. Bereits frühzeitig wurde das RSA-Verfahren ¹ als geeignetster Signieralgorithmus gewählt und erkannt, daß die sichere Speicherung der geheimen Schlüssel auf Prozessorchipkarten erfolgen soll. Solche sind bereits zu adäquaten Preisen verfügbar und gerade der Bankenbereich verfügt über langjährige Erfahrung damit und die entsprechenden logistischen Einrichtungen. Die große Zahl an Geschäftsstellen ermöglicht eine flächendeckende Versorgung sowie einen für den Kunden einfachen Bestell- und Registrierungsvorgang.

Die hohen sicherheitstechnischen Anforderungen ergaben sich schon aus dem Bedürfnis der Banken, aber auch aus der Überlegung, daß die rechtliche Anerkennung der bankmäßigen Signaturen eine wesentliche Voraussetzung für eine breite Anwendungspalette darstellt. Da es hierzu keine einschlägigen Vorschriften in Österreich gab und gibt, orientierte man sich am damals entstehenden deutschen Signaturgesetz, welches sehr strenge Maßstäbe anlegt. Parallel wurde Kontakt mit Ministerien aufgenommen, welche sich mit dieser Materie befassen, um inhaltlich und zeitlich mit den kommenden rechtlichen Anforderungen konform gehen zu können. Nachdem die Machbarkeitsstudie die Schaffung eines solchen Systems auch aus betriebswirtschaftlicher Sicht empfehlenswert erscheinen ließ, wurde die Realisierung in zwei Projektteams beschlossen: In Verantwortung der STUZZA wurden Detailspezifikationen ausgearbeitet. Darauf basiert die nun bereits in Angriff genommene Entwicklung in Verantwortung der APSS (Austrian Payment Systems Services, ebenfalls ein Tochterunternehmen der österreichischen Banken, bekannt als Bankomat-Betreiber), welche in der Folge als gemeinsame Zertifizierungsinstanz (ZI) für die Banken auftreten wird. Die technische Abnahme wird wiederum in Verantwortung der STUZZA erfolgen. Damit wird eine durchgängige und nachvollziehbare Funktionsteilung zwischen Konzept und Realisierung sowie die Konsistenz mit den Vorgaben gesichert. Das fertige System wird dann einer unabhängigen Sicherheitsevaluierung unterzogen, für deren exakte Anforderungen die entstehenden Rechtsvorschriften und Zuständigkeiten abzuwarten sind. Der Terminplan sieht vor, daß ab Mitte 1999 funktionierende Chipkarten ausgegeben werden können und Digitale Signaturen entgegengenommen werden können. Multibankfähige Electronic Banking Anwendungen (MBS-Standard) werden das erste Einsatzgebiet darstellen. Ursprünglich erwogen wurde ein gemeinsamer Start mit der Umstellung der Electronic Banking Systeme auf den Euro. Schließlich entschied man sich dann aufgrund des damit verbundenen hohen Terminrisikos für eine zeitliche Entflechtung.

Projektumfang

Die generellen Zielsetzungen leiten sich aus den dargestellten Prämissen, allen voran Sicherheit, Interoperabilität und rechtliche Anerkennung ab. Der Projektumfang wird begrenzt von der Unterscheidung zwischen sinnvollerweise gemeinsam zu errichtender Basisinfrastruktur zum Unterschied von darauf aufbauenden Produkten, welche Unterscheidungsmerkmale zwischen den Instituten im Wettbewerb enthalten sollen. Das Projekt umfaßt somit den "Werkzeugkasten" für die Digitale Signatur, aber nicht die unmittelbare Anwendung selbst. Eine Mittelstellung nehmen dabei solche Applikationen ein, welche nur aus gemeinsamer Sicht einen Sinn ergeben, wie etwa der Datenaustausch zwischen den Banken untereinander.

¹ nach seinen Erfindern Rivest Shamir Adleman benannt.

Die wichtigsten Funktionen

Signieren einer Nachricht im Electronic Banking

Das Anwendungsprogramm bietet den gewohnten Arbeitsablauf, z.B. Erfassen und Kontrollieren von Zahlungsaufträgen. Vor dem Absenden an die Bank wird der Benutzer aufgefordert, seine Chipkarte einzulegen und seine PIN einzutasten. Es wird nun der Hash-Wert (kryptographische Prüfsumme) über die Auftragsdatei gebildet und an die Chipkarte geleitet. Diese verknüpft nun den geheimen Schlüssel mit dem Hash-Wert; es entsteht die Signatur für diesen Auftrag und wird an die Anwendung übergeben, welche sie gemäß dem verwendeten Datenformat anhängt bzw. einfügt und das Ganze an den Empfänger absendet. Mehrfachzeichnungen werden realisiert, indem dieser Vorgang entsprechend oft von unterschiedlichen Zeichnungsberechtigten wiederholt wird.

Verifizieren einer Signatur durch die Bank

In einem vollautomatischen Ablauf wird stufenweise die Gültigkeit geprüft: Zunächst wird das zugehörige Zertifikat aus dem Directory Service (DS) der Zertifizierungsinstanz (ZI) abgefragt und die Signatur mit dem öffentlichen Schlüssel entschlüsselt. Ergebnis sollte der Hash-Wert (kryptographische Prüfsumme) laut Nachricht sein. Dieser wird nun nachvollzogen, indem er aus der vorliegenden Nachricht nochmals gebildet wird. Bei Übereinstimmung ist die Signatur richtig und die Nachricht muß unverfälscht angekommen sein. Nun wird geprüft, ob das Zertifikat gültig ist und ob kein Widerruf anhand der Sperrliste vorliegt. Ist das Ergebnis o.k., dann liegt eine völlig korrekte Signatur vor. Auch dieser Vorgang wird im Fall von Mehrfachzeichnungen wiederholt.

Danach erfolgt die bankmäßige Prüfung, die bereits jenseits des Signaturmechanismus liegt: Haben alle und die richtigen Zeichnungsberechtigten laut Kontonummer signiert, liegt die notwendige Deckung vor, u.s.w.

Was bei Fehlersituationen zu geschehen hat, obliegt der empfangenden Bank. Im Falle einer regelmäßigen Geschäftsverbindung wird zunächst meist beim Kunden rückgefragt werden.

Bestellung einer Signaturkarte und Registrierung

Vom Prinzip her muß sichergestellt werden, daß eine Signaturkarte samt Zertifikat nachweislich mit einer bestimmten Person verknüpft wird. Der übliche Ablauf wird eine schriftliche Bestellung (etwa ein elektronisches Formular im Internet) an die kontoführende Geschäftsstelle der Hausbank vorsehen. Aufgrund der ausgefüllten Daten veranlaßt diese einen Bestelldatensatz an die Zertifizierungsinstanz (ZI), welche eine Zertifikatsnummer vergibt und die Produktion der Karte auslöst. Der Kartenproduzent versendet die Karte an die bestellende Geschäftsstelle, das zugehörige PIN-Kuvert an den Kunden sowie den passenden öffentlichen Schlüssel zurück an die ZI.

Nach Erhalt des PIN-Kuverts muß der Kunde seine Karte persönlich in der Geschäftsstelle abholen und sich dabei ausweisen. Der Mitarbeiter der Geschäftsstelle ist persönlich verantwortlich, daß er den Ausweis geprüft hat und ein Nachweis (Kopie in einem sicher verwahrten Kundenakt) darüber existiert. Er übergibt dem Kunden die Karte und löst einen weiteren Datensatz über die Tatsache der erfolgten Abholung an die ZI aus. Die ZI macht nun das zugehörige Zertifikat im Verzeichnis gültig.

Diese Organisationsform hat den Vorteil, daß der Kunde nur einmal persönlich vorsprechen muß. In Kauf zu nehmen ist eine gewisse zeitliche Verzögerung der Gültigwerdung abhängig vom Weg der Datensätze an die ZI.

Hat man nun Karte und PIN in Händen, muß zunächst als zwingende Sicherheitsmaßnahme die PIN laut Kuvert auf einen selbstgewählten Wert geändert werden.

Ausnahmefälle

PIN-Fehler: Nach dreimaliger Fehleingabe ist die Signaturkarte gesperrt. Der Kunde hat die Möglichkeit, diese Sperre mit Eingabe einer PUK (PIN Unblock) wieder aufzuheben. Die PUK ist eine separate Geheimzahl, welche mit dem PIN-Kuvert mitgeliefert wird (wie beim GSM-Mobiltelefon). Allerdings gibt es keine Möglichkeit, eine endgültig vergessene PIN in irgendeiner Form zu rekonstruieren. In einem solchen Fall muß eine neue Signaturkarte bestellt werden. Selbstverständlich ist auch die Zahl der möglichen PUK-Eingaben beschränkt.

Sperre bei Verlust oder Diebstahl der Signaturkarte: Kann sich ein Unbefugter in den Besitz von Karte und PIN bringen, dann kann er im Namen des rechtmäßigen Inhabers beliebig rechtswirksame Signaturen leisten. Dies muß mit geeigneten Maßnahmen verhindert werden. Bei entsprechendem Verdacht kann man zunächst eine temporäre Sperre (Suspension) telefonisch oder schriftlich (Fax) bei der ZI veranlassen. Da das einfach und schnell möglich sein muß, sind keine besonderen Überprüfungen möglich. Ausgelöst wird ein entsprechender Eintrag ins Zertifikatsverzeichnis und die Sperrlisten, ab dann geleistete Signaturen sind - auch rechtlich - ungültig. Zum Schutz vor mißbräuchlichen Sperren wird eine solche Suspension nach mindestens 24 Stunden, d.h. am darauf folgenden Bankwerktag, wieder aufgehoben. Bis dahin muß man entweder die Karte wieder gefunden haben oder einen dauerhaften Widerruf (Revocation) veranlassen. Dieser kann jedoch nur von der ausstellenden Geschäftsstelle veranlaßt werden, da diese im Besitz der Identitätsnachweise ist. Wesentlich ist dabei, daß sich der Widerruf nicht auf vorher geleistete Signaturen bezieht. Dies impliziert für den Empfänger, daß er sich von der Aktualität der Zertifikate überzeugen muß. Für den Signierenden bedeutet es, bei Verdacht auf Verlust oder Diebstahl rasch zu handeln.

Designkriterien

Signier- und Hash-Algorithmen

Als Signieralgorithmus wurde der RSA ausgewählt. Er ist für den Zweck optimal geeignet, weiters als internationaler de-facto Standard in Form von Produkten ausreichend verfügbar und konnte seit 15 Jahren nicht gebrochen werden. Seine Nachteile wie die relativ langen Schlüssel sowie die nach wie vor bestehenden US-Exportbeschränkungen mußte man in Kauf nehmen, da sich insgesamt keine überlegenen Alternativen ergaben. Als für mehrere Jahre zukunftssichere Schlüssellänge wurden 1024 bit festgelegt.

Eine weltweite Normierung einer einzigen Hash-Funktion für Zwecke der elektronischen Unterschrift ist nicht abzusehen, es werden vielmehr unterschiedliche Verfahren herangezogen (Internet: SHA-1, MD5, Deutsche Banken: RIPEMD-160). Dementsprechend müssen flexibel verschieden Hash Algorithmen verwendet werden können.

Signaturkarte (Chipkarte)

Da die Sicherheit des Verfahrens für den Benutzer in der Geheimhaltung seines privaten Schlüssels liegt, wurde dessen softwaremäßige Verwahrung auf Festplatten, Disketten, u.s.w. bereits frühzeitig verworfen und Chipkarten als geeignete Medien spezifiziert. Der private Schlüssel wird im Zuge der Produktion innerhalb des Chip erzeugt und verläßt ihn niemals. Nur damit kann ausgeschlossen werden, daß manipulierte Programme wie Viren den privaten Schlüssel auslesen und in der Folge beliebige Signaturen unbemerkt erzeugen können. In gleicher Weise wird ein unbefugtes Auslösen des Signiermechanismus verhindert, da sich dieser ebenfalls auf der Chipkarte befindet und nur mittels der gültigen, selbstgewählten PIN aktiviert werden kann. Dies impliziert allerdings, daß der Benutzer seine Chipkarte und PIN sicher verwahrt und niemandem anderen übergibt. Biometrische Mechanismen zur Aktivierung der Chipkarte wären hier sicher wünschenswert, zur Zeit gibt es aber noch nicht ausreichend preislich vergleichbare Produkte. Positiver Effekt der Chipkarte ist weiters die einfache Möglichkeit, den Schlüssel dorthin mitzunehmen, wo man ihn einsetzen will.

Aufgrund der fundamentalen Bedeutung für die Sicherheit stellt gerade die Spezifikation der Chipkarte sehr hohe Ansprüche und fordert entsprechende Sicherheitszertifizierungen des Chip, Betriebssystems, Signaturmechanismus sowie des Initialisierungs- und Personalisierungsvorgangs, d.h. des korrekten Ladens der Software in den Chip.

Zertifikate und Zertifizierungsinstanz (ZI)

Zertifikate entsprechen der weltweiten Norm ISO 9594_8 (besser bekannt als X.509) und beinhalten zum einen den zu einer bestimmten Person gehörenden passenden öffentlichen Schlüssel, zum anderen stellen sie ihren "elektronischen Ausweis" dar. Dieser bildet sich aus Daten zur eindeutigen Identifikation und Gültigkeit sowie der digitalen Signatur des Ausstellers, genannt Zertifizierungsinstanz (ZI). Die ZI bürgt und haftet also dafür, daß ein bestimmter öffentlicher Schlüssel eindeutig einer bestimmten Person zugeordnet ist, welche über den passenden privaten Schlüssel verfügt und daß der Zeitpunkt der Erstellung korrekt dargestellt ist.

Aus dieser zunächst einfach erscheinenden Funktion ergeben sich eine Fülle von technischen und organisatorischen Anforderungen sowie eine hohe Verantwortung:

Der kritischste Vorgang ist die Ausstellung eines Zertifikats. Die ZI muß sicher sein, daß nur korrekte Grunddaten des Benutzers zertifiziert werden. Sie erhält diese von den Geschäftsstellen, welche die Identifikation der Besteller durchführen. Die ZI muß ihnen den jeweils passenden öffentlichen Schlüssel zuordnen. Er entsteht im Produktionsprozeß der Chipkarten. Weiters ist ein Zeitstempel erforderlich, auf dem der Gültigkeitszeitraum basiert. Schließlich muß die ZI ihre eigene Signatur anbringen, d.h. das Rohzertifikat mit Hilfe ihres geheimen Schlüssels signieren. Es muß sichergestellt und nachweisbar sein, daß keiner der Abläufe unbefugte Manipulationen zuläßt. Am sensibelsten ist der geheime Schlüssel der ZI selbst; bei seiner Kompromittierung könnten beliebige gefälschte Zertifikate ausgegeben werden. Daher wird seine Erstellung und Speicherung in einem Hochsicherheitsmodul gefordert, welches er niemals verlassen darf.

In der **konkreten Spezifikation** wurde nach Vorbild der Bankomatkarten eine praktische Umsetzung konzipiert: Die Abwicklung der Bestellung erfolgt durch die Geschäftsstelle der Bank und liefert zunächst Grunddaten an die Banken-ZI. Es wird davon ausgegangen, daß der Kunde bei einer

Bank bestellt, bei der ein Konto hat, also die Bezahlung der Chipkarte und des Zertifikats gesichert ist. Die Banken-ZI vergibt eine Zertifikatsnummer und beauftragt den Kartenhersteller mit der Produktion aufgrund dafür mitgelieferter Daten. Im Zuge der Produktion wird die Karte hergestellt, d.h. innerhalb des Chip ein geheimer sowie öffentlicher Schlüssel generiert und die Zertifikatsnummer aufgeprägt. Der öffentliche Schlüssel geht per Datenträger zurück an die ZI, die fertige Karte an die gewünschte Geschäftsstelle.

Directory Service (DS)

Es handelt sich dabei um das elektronische Verzeichnis aller von der ZI ausgegebenen Zertifikate. Man kann es sich wie ein Telefonbuch vorstellen, mit der Suche nach dem gewünschten Namen eines Schlüsselinhabers erhält man dessen Zertifikat, damit also seinen öffentlichen Schlüssel. Empfänger von Digitalen Signaturen können Zertifikate entweder einzeln abfragen oder bei regelmäßiger Geschäftsverbindung bei sich vorhalten. Zertifikate als solche können beliebig verteilt werden, da sie mittels der Signatur der ZI fälschungssicher sind.

Kritisch ist der Änderungsdienst am Zertifikatsverzeichnis, daher wird dieser zweckmäßig ausschließlich durch die ZI erfolgen. Es muß sowohl sichergestellt sein, daß keine unbefugten Veränderungen möglich sind, aber auch daß jeweils der aktuellste Stand für alle Teilnehmer verfügbar ist. Besondere Bedeutung kommt der Gültigkeit eines Zertifikats zu: Sein Inhaber muß in der Lage sein, sie im Falle des Diebstahls, Verlustes seiner Karte oder aus anderen Gründen zu widerrufen. Signaturen, welche ab diesem Zeitpunkt mit seinem Schlüssel erzeugt werden, sind ungültig. In der Praxis ist daher ein Sperrmanagement ähnlich der Bankomatkarte vorzusehen:

Ein neu erstelltes Zertifikat ist grundsätzlich gültig, bis seine Gültigkeitsperiode abläuft (dzt. 3 Jahre). Danach muß eine neue Chipkarte und ein neues Zertifikat erzeugt werden. Bei Verdacht auf Verlust oder Diebstahl kann sein Inhaber zunächst eine sog. Suspension bei der ZI veranlassen (telefonisch oder per Fax). Damit wird die Gültigkeit vorübergehend (bis zum Ende des nächsten Bankwerktags) aufgehoben. Geschieht nichts weiter, dann wird das Zertifikat automatisch wieder gültig. Dies zum Schutz vor böswilligen Sperren durch Unbefugte. Stellt sich tatsächlich Verlust oder Diebstahl heraus, dann ist der Widerruf (Revocation) beim ausgebenden Bankinstitut zu veranlassen, womit das Zertifikat dauerhaft ungültig wird.

Jede dieser Änderungen bedarf einer Eintragung im Verzeichnis. Es ist klar, daß an die schnelle Abwicklung und Korrektheit hohe Anforderungen zu stellen sind, da von der Aktualität des Verzeichnisses wesentliche Rechtsfolgen abhängig sind. Es obliegt dem Empfänger einer Signatur, zu prüfen ob das Zertifikat gültig bzw. nicht widerrufen ist. Dies wird ihm durch die abrufbare "Revocation List" erleichtert, welche alle aktuellen Sperren enthält. Ihre Kommunikation erfordert ein sicheres Übertragungsprotokoll, damit sie nicht auf dem Weg unbefugt manipuliert werden kann.

Stand der rechtlichen Rahmenbedingungen

Viele Rechtsordnungen, darunter auch die österreichische, kennen den Begriff der Digitalen Signatur noch nicht. Ausgesprochene Signaturgesetze gibt es in Europa in Deutschland und Italien. Auch diese decken allerdings noch nicht das Gesamtszenario ab, dessen Ziel es ist, mit Digitalen Signaturen unmittelbare Rechtsfolgen eindeutig zu verknüpfen. Ein Problem dabei ist es, im Bereich einer sich rasant entwickelnden Technologie angemessene Sicherheit zu definieren. Gesetzliche Regelungen

müssen in ausgewogener Weise die Bedürfnisse des Signierers und des Verifizierers berücksichtigen, gleichzeitig den Zertifizierungsinstanzen die wirtschaftlich sinnvolle Tätigkeit ermöglichen und zudem international harmonisiert sein.

Entwurf einer EU-Richtlinie

Im Rahmen einer Initiative zur Förderung des elektronischen Geschäftsverkehrs wurde im Mai 1998 ein Richtlinienentwurf der Europäischen Kommission² veröffentlicht, welcher in den Mitgliedsstaaten laut Planung bis Ende 2000 umzusetzen ist. Inhaltlich ist der Rahmen über die Digitalen Signaturen hinaus sehr weit gesteckt und soll von der Zielsetzung her auch biometrische Verfahren abdecken. Daher hat man im Entwurf neue Begriffe eingeführt. In den Details wird allerdings hauptsächlich auf Zertifizierungsdienste für Digitale Signaturen eingegangen. Signifikant ist, daß die rechtliche Gleichstellung der "elektronischen Signaturen" mit manuellen Unterschriften gefordert wird, sofern "qualifizierte Zertifikate" ausgestellt von geeigneten "Zertifizierungsdiensteanbietern" zur Anwendung kommen. Die Anforderungen an Zertifikate und Zertifizierungsdiensteanbieter sind in jeweils eigenen Anhängen - allerdings in sehr genereller Weise - angeführt. Genaue Anforderungen an die zu verwendende Technik fehlen noch, wurden jedoch im Zuge der Begutachtung von einigen Mitgliedsländern - auch von Österreich - eingebracht.

Klar ausgesagt wird, daß es keine behördliche Zulassung für "Zertifizierungsdiensteanbieter" geben soll, sondern eine freiwillige Akkreditierung. Dafür sind ausführliche Haftungsregelungen für solche Betreiber definiert.

Die derzeitige Version ist in einigen Punkten umstritten, vor allem die Situation daß den erheblichen Rechtsfolgen Digitaler Signaturen eine nur ansatzweise geregelte Palette von Produkten und Betreibern gegenübersteht, deren Sicherheit und Qualität der Anwender kaum nachvollziehen kann. Mancherorts wird eine Flut an Zivilprozessen hinsichtlich Haftung befürchtet. Ob die Richtlinie wie geplant im November 1998 verabschiedet wird, ist somit heute schwer abzuschätzen.

Österreichische Gesetzeswerdung

Zur Zeit können digitale Signaturen im Rahmen der Vertragsfreiheit ohne weiteres eingesetzt werden. Das heißt, im Rahmen bestehender Geschäftsbeziehungen kann von Rechtssicherheit ausgegangen werden. Die Grenzen liegen dort, wo besondere Formvorschriften gelten, in der Praxis z.B. im Umgang mit Behörden oder bei Geschäften zwischen einander Unbekannten. Weiters hat man das Problem, daß es Sicherheits- oder Qualitätskriterien nicht festgelegt bzw. nachvollziehbar sind und man als Benutzer praktisch dem Betreiber vertrauen muß.

Eine Gesetzesinitiative wurde für 1998 angekündigt und ministerielle Vorarbeiten geleistet. Mit der Ankündigung der EU-Richtlinie macht es allerdings erst nach ihrer Verabschiedung Sinn, konkrete nationale Gesetze zu erlassen, da sie damit konform gehen müssen.

Zur Zeit **bekannt Positionen** österreichischer **Regierungsstellen** sind dazu:

- Gesetzliche Regelungen für Digitale Signaturen sollen nur in Verbindung mit konkreten Rechtsfolgen erlassen werden. Als erster Schritt kann dann für derart signierte elektronische

² "Gemeinsame Rahmenbedingungen für elektronische Signaturen vom 13.5.1998

Dokumente die Echtheitsvermutung gelten, d.h. der Empfänger muß im Disputfall Zweifel an der Echtheit nachweisen. De facto bedeutet dies die Anerkennung durch Behörden.

- Signaturen, welche den Anspruch auf Rechtsfolgen stellen, müssen von der Technik und Zertifizierung gesetzlichen Anforderungen genügen. Da die EU-Richtlinie eine behördliche Zulassung ausschließt, wird voraussichtlich eine amtlich anerkannte Aufsicht installiert werden. Ihre Aufgabe wird es sein, Anforderungen an Produkte und Betreiber zu entwickeln und zu kontrollieren.
- Sonstige Systeme im Rahmen bestehender Verträge sollen davon nicht berührt werden.

Position der Kreditinstitute: Sie sind in erster Linie Anwender, da sie empfangene Signaturen von ihren Kunden verifizieren und in der Folge Zahlungsaufträge ausführen müssen. Künftig ist eine Ausweitung auf Wertpapieraufträge bzw. sonstige Dienstleistungen zu erwarten, welche heute einer manuellen Unterschrift des Kunden bedürfen. Da erhebliche Geldwerte bewegt werden bzw. rechtliche Verantwortungen eingegangen werden, dürfen keine Sicherheitsrisiken entstehen. Abgesehen von materiellen Schäden könnte bei unzureichender Sicherheit auch das Image der Banken als vertrauenswürdige Partner nachhaltig beschädigt werden. Dies ist der Grund, warum sich die Institute entschlossen haben, für ihre Dienstleistungen eine entsprechende Infrastruktur zu errichten und dabei höchsten Sicherheitsansprüchen zu genügen; etwa mittels Chipkarten. Daher ist das Design so ausgelegt, die kommenden Rechtsvorschriften zu erfüllen und somit auch behördlich anerkannte Zertifikate anzubieten. Damit wird der Benutzer eine ausreichend attraktive Angebotspalette vorfinden.

Ungeachtet ihres Bekenntnisses zum freien Wettbewerb - auch zwischen künftigen Zertifizierungsinstanzen - wird man es den Instituten nicht zumuten können, Digitale Signaturen zu akzeptieren, wenn sie von deren Sicherheit nicht überzeugt sind. Daher sind klare, hinreichend exakte und nachvollziehbare Sicherheitsanforderungen sowie Prozeduren zu ihrem Nachweis zu fordern - ein Anliegen, dem sich auch die Notenbank anschließt.

Absehbare Perspektiven

Vom Standpunkt des Benutzers sind rechtsgültige Digitale Signaturen dann attraktiv, wenn sie ihm generell ermöglichen, Papierdokumente durch elektronische Medien zu ersetzen. Die Bedürfnisse reichen weit über Banktransaktionen hinaus, etwa zu elektronischen Bestellungen aller Art, die Bestätigung des Erhalts "eingeschriebener E-Mails", über elektronische Verträge mit der Signatur eines Notars bis hin zum elektronischen Antrag an eine Behörde und dessen Erledigung über das Internet. Gelingt es in absehbarer Zeit ein umfassendes Anwendungsgebiet anzubieten, dann werden Digitale Signaturen zu einem nicht mehr wegzudenkenden Werkzeug und die letzte große Lücke zur papierlosen Kommunikation schließen.

Unbeschadet dieser Szenarien wird ein ebenso attraktiver Markt für Signaturen und Zertifikate entstehen, welche nur speziellen Anforderungen genügen müssen. Beispiele dafür sind bereits jetzt angebotene spezialisierte Zahlungssysteme sowie die Sicherung gegen Übertragungsmanipulationen bzw. -fehler bei technischen Zeichnungen in Intranets. Hier bestehen ja bereits etablierte Verbindungen zwischen den Kommunikationspartnern.

Als wichtigstes Anliegen ist die baldige Schaffung der umfassenden Rechtssicherheit zu nennen, da hohe Investitionen auf dem Spiel stehen und in Österreich, aber auch in Europa zur Zeit auf diesem Gebiet ein deutlicher Technologievorsprung besteht. Es geht hier nicht um neue Vorschriften, sondern um klare und verständliche Spielregeln. Wenn man zuwartet, bis globale Standardlösungen auf dem Markt sind, dann werden das wohl kaum österreichische, aber vermutlich auch nicht europäische sein.

Die zweite wesentliche Voraussetzung für die breite Akzeptanz ist die Bewußtseinsbildung in der Öffentlichkeit. Heute kann man nicht davon ausgehen, daß Digitale Signaturen und ihre Möglichkeiten flächendeckend bekannt sind. Dies gilt in gewissem Ausmaß auch für Chipkarten - einem Medium mit dem voraussichtlich bald jeder krankenversicherte Österreicher konfrontiert sein wird. Hier gilt es, verstärkt fundierte und ehrliche Information zusammenzutragen und zu verteilen.

Zum Autor:

Manfred Holzbach,

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

Quick im Internet

Quick Classic

Smartcards sind in ihren Anwendungsmöglichkeiten schier unerschöpflich. Eine dieser Anwendungsmöglichkeiten - und durchaus eine der besten - ist die elektronische Geldbörse. Dies zeigt seit 1995 das österreichische System namens "Quick".

Quick wurde unter der Federführung der Europay Austria/APSS entwickelt und wird von dieser auch betrieben. Es begann bereits 1995, als in einem Feldversuch in Eisenstadt die Einsatzmöglichkeiten und wirtschaftliche Positionierung dieses zukunftsweisenden Zahlungsmittels abgetestet wurden. Nach diesem Feldversuch und einem im Frühjahr 1996 gestarteten weiteren Pilotbetrieb in fünf Vorziehstädten ging Quick im Oktober 1996 österreichweit in Echtbetrieb.

Die rasch wachsende Infrastruktur bestand schon Ende 1997 aus über 12.000 Zahlungsterminals und 3700 Ladeterminals, an denen man die Quickkarte gegen Bargeld oder Bankomatbelastung aufladen konnte. Derzeit stehen rund 16.500 Zahlungsterminals und 4.400 Ladeterminals zur Verfügung.

... ist erst der Anfang ...

Quick ist stark in Richtung kleiner Beträge ausgerichtet. Das hat seinen Grund vor allem im praktischen und schnellen Bezahlvorgang, dem Ladebereich bis 1.999,- ATS und dem für die Kunden wegfallenden Problem der Kosten pro Buchungszeile. Bei Quick werden nur die Ladevorgänge mit je einer Buchungszeile verbucht.

Österreichweit sind über 3,5 Mio. ec- bzw. Bankomatkarten im Umlauf, dazu kommen noch die anonymen Quick-Wertkarten und seit 7/98 rund 100.000 BIPA-Best-Cards.

All diese Faktoren machten aus Quick ein starkes Zahlungsverkehrsprodukt für den Einsatz in Geschäften. Für diesen Bereich wurde das Handling von geringen Beträgen eindeutig erleichtert.

Auftritt Internet

Aber nicht nur im "realen" Leben gibt es den Bedarf nach praktischen, billigen und sicheren Zahlungsmitteln. Das Internet entwickelte sich im Laufe der letzten vier Jahre vom reinen Wissenschafts- und Forschungsnetz der siebziger und achtziger Jahre zum allumfassenden Informations- und Wirtschaftsdatennetz.

Die Zahl der am Internet teilnehmenden Computer boomt, und die Zahl der Benutzer steigt so rasch, daß sich alle Statistiken bereits nach wenigen Wochen überholt haben. Wenn sogar schon die PTA mit dem Popsänger *Ostbahnkurti* "des Intanetz" bewirbt, wenn sich Boulevardmagazine wöchentlich mit den "besten Webseiten" aus dem Internet überschlagen und wenn der ORF

formatfüllend seine Chat-Seiten anpreist, kann man ersehen, wie sehr das Internet schon Teil der Allgmeinkultur und des Lebensumfeldes der Österreicher geworden ist.

Das Internet ist Teil des öffentlichen Raums geworden. Hier präsentieren sich Firmen, werben neue Kunden, betreuen die bestehenden schneller und direkter, stellen ihre Produkte vor und eröffnen sich durch das Internet vollkommen neue Vertriebsmöglichkeiten. Nicht zuletzt durch den Einsatz des Internets wurde *Dell* in kürzester Zeit zu einem der Major Players auf dem hartumkämpften PC-Markt, und nicht umsonst zittert der amerikanische Buchhandel vor *amazon.com*, einem nur über das Internet auftretenden Buch-Direktversand.

Zahlen übers Internet

Der Markt ist also scheinbar schon da: Die Anbieter befinden sich schon seit einiger Zeit im Internet, die Kundschaft wären auch schon da, allein es fehlt am Geld. Und zwar genauer gesagt, an einer Art Geld, das im Bereich Internet sicher, einfach und kostengünstig für Zahlungen verwendet werden kann.

Es gibt Software, mittels derer anbietende Firmen ihre Produkte leicht und auf ansehnliche Weise im Internet präsentieren können. Diese wird Merchantserver oder auch Commercserver genannt. Ein Merchantserver verwaltet einerseits die Webseiten, die sogar halbautomatisch aus dem Artikelstamm erstellt werden können, und andererseits auch den Auftragseingang und die Kunden. Ein Kunde kann dieses "Online-Geschäftslokal", das der Merchantserver im Internet repräsentiert, per Browsersoftware (Netscape Navigator, Internet Explorer o.a.) durchwandern. Will er dann tatsächlich etwas kaufen, muß i. a. zuerst die Zahlung stattfinden, und danach geht die Ware auf dem gewünschten Lieferweg gleich an den Kunden. Dies kann der gewohnte Post- oder Speditionsweg bei herkömmlichen Waren sein; für elektronische Waren, wie z. B. Software, kostenpflichtige Informationen, Dateien, Grafiken, Filme, Musik usw. oder auch Dienstleistungen (kostenpflichtiger Helpdesk, Online-Arbeiten wie Fernkonfiguration o. ä.) bietet sich natürlich als schnellster Lieferweg auch gleich die Versendung bzw. Leistung übers Internet an. Dieses Prinzip der "Instant gratification", also der sofortigen Verwendbarkeit, wird von den Online-Kunden in vielen Fällen als Grundvoraussetzung für einen Kauf angesehen.

Die bereits bestehenden und verwendeten Zahlungsmittel haben allerdings einige Nachteile. So wird die Bezahlung durch die technisch ungesicherte Übermittlung der Kreditkartennummer übers Internet von den Onlineshoppern aus Sicherheitsgründen abgelehnt. Der Standard "SET" für das sichere Bezahlen mit Kreditkarte im Internet befindet sich in Österreich bei Mastercard/Eurocard und VISA dzt. bereits in der Pilotphase, jedoch werden damit vorzugsweise größere Beträge bezahlt. Andere Systeme haben das Problem, daß sie noch relativ wenig verbreitet sind. Weitere Nachteile sind die durchwegs hohen Kosten, die bei diesen Systemen für Kunden und Händler anfallen (z. B.: Ecash mit Händlergebühren von 4200 ATS einmalig plus 2,5% Disagio plus monatlicher Händlergebühr plus Gebühren für den Kunden; Kreditkarten bis zu 4% Disagio händlerseitig plus Kundengebühren). Stark verlangt wird von den Onlinekunden bei einigen Geschäftstypen auch die Anonymität der Zahlung, also daß bei der Zahlung nicht auf den Bezahler rückgeschlossen werden kann.

Quick im Internet : Die drei Teile

Hier kann das System "Quick im Internet" seine Vorteile ausspielen. Es ist das derzeit am sichersten vorstellbare System. Es ist anonym, d.h. daß bei einer Zahlung weder Kontonummer, Bankleitzahl oder Name der Karteninhaber dem Händler bekanntgegeben werden, es ist einfach und benutzerfreundlich anzuwenden, und es ist weit verbreitet (über 3 Mio. Karten in Österreich).

Bei "Quick im Internet" spielen drei Teile mit: der Merchantserver, der Bezahlserver und die Kundensoftware. Eine schematische Darstellung ist in Abbildung 1 zu sehen.

Merchantserver, ...

Als Merchantserver kann jeder beliebige auf dem Markt befindliche Merchantserver verwendet werden, für den ein sogenanntes Quick-Modul zur Verfügung steht. Dieses Quick-Modul ist eine Erweiterung der jeweiligen Merchantserver-Software, damit diese auch Quick-Zahlungen und die Kommunikation mit dem Quick – Bezahlserver beherrscht. Ein solches Quick-Modul für den jeweils gewünschten Merchantserver kann unter technischer Hilfestellung der APSS und nach einer von der APSS veröffentlichten Schnittstellenbeschreibung von seiten des Händlers hergestellt werden. Dies ist für ein laufendes Merchantserver-System technisch äußerst einfach. Die APSS kann an interessierte Händler auf Wunsch aber auch Quick-Module für die gängigsten Merchantserver ausliefern. Derzeit als Referenzsystem vorhanden ist ein Quick-Merchantmodul für den Minivend-Merchantserver. In Entwicklung sind Quick-Merchantmodule für den Intershop- und den Oracle-Merchantserver, andere sind in Planung. Der Quick-Merchantserver des Händlers befindet sich dann wie jeder andere normale Merchantserver beim jeweiligen Händler.

...Bezahlserver samt Terminalkarten, und...

Der Bezahlserver, auch Paymentsserver genannt, ist ein Server, der bei der EPA/APSS steht und sämtliche "Quick im Internet"-Bezahlungen abwickelt. Jede derzeitige Quickzahlung im "klassischen Quick" ist in Wahrheit eine Bezahlung von der Quick-Kundenkarte auf die sogenannte "Händlerkarte" (auch Terminalkarte genannt). Diese Händlerkarte ist bei den Händlerterminals (die in den letzten ASA-News vorgestellt wurden) ins Gerät eingebaut. Das heißt, jede Quick-Bezahlung ist eine Abbuchung von der Quick-Kundenkarte mit nachfolgender Aufbuchung auf die (versteckte) Quick-Terminalkarte. Dieses Prinzip wird natürlich beim Quick im Internet beibehalten: Hier ist für jeden Händler eine bestimmte Anzahl von Terminalkarten vorgesehen, welche alle an den Bezahlserver angeschlossen sind.

Dafür benötigt man eine große Anzahl Kartenleser, da ja alle Terminalkarten aller Händler zur gleichen Zeit verfügbar sein müssen. Zum Anschluß dieser (derzeit noch zweistelligen) großen Anzahl Kartenleser an den einen Bezahlserver wird ein Terminalserversystem der Firma Cyclades verwendet, das auf bis zu mehrere hundert Anschlüsse für Kartenleser ausgebaut werden kann. Eine quasi unbeschränkte Anzahl läßt sich durch die Verwendung eines sogenannten ASM erreichen, der jedoch erst im kommenden Jahr zur Verfügung stehen wird.

Jeder Händler hat also heute eine bestimmte Anzahl eigener Terminalkarten. Diese sind ähnlich aufzufassen wie die üblichen Quick-Händlerterminals – mit einer Terminalkarte kann natürlich nur immer eine Zahlung zugleich abgewickelt werden. Vor allem zu den "Stoßzeiten" (früher Abend) sollte also sichergestellt werden, daß genügend Terminalkarten für die Kunden verfügbar sind.

... die Kundensoftware

Neben einem normalen Browser verwendet der Kunde einen Kartenleser und die Quick-Client-Software. Diese Software läuft am PC des Kunden im Hintergrund und wickelt die wirkliche Quick-Transaktion ab, welche ja zwischen der Kundenkarte im Kunden-Kartenleser und der Terminalkarte am Bezahlserver in der APSS stattfindet.

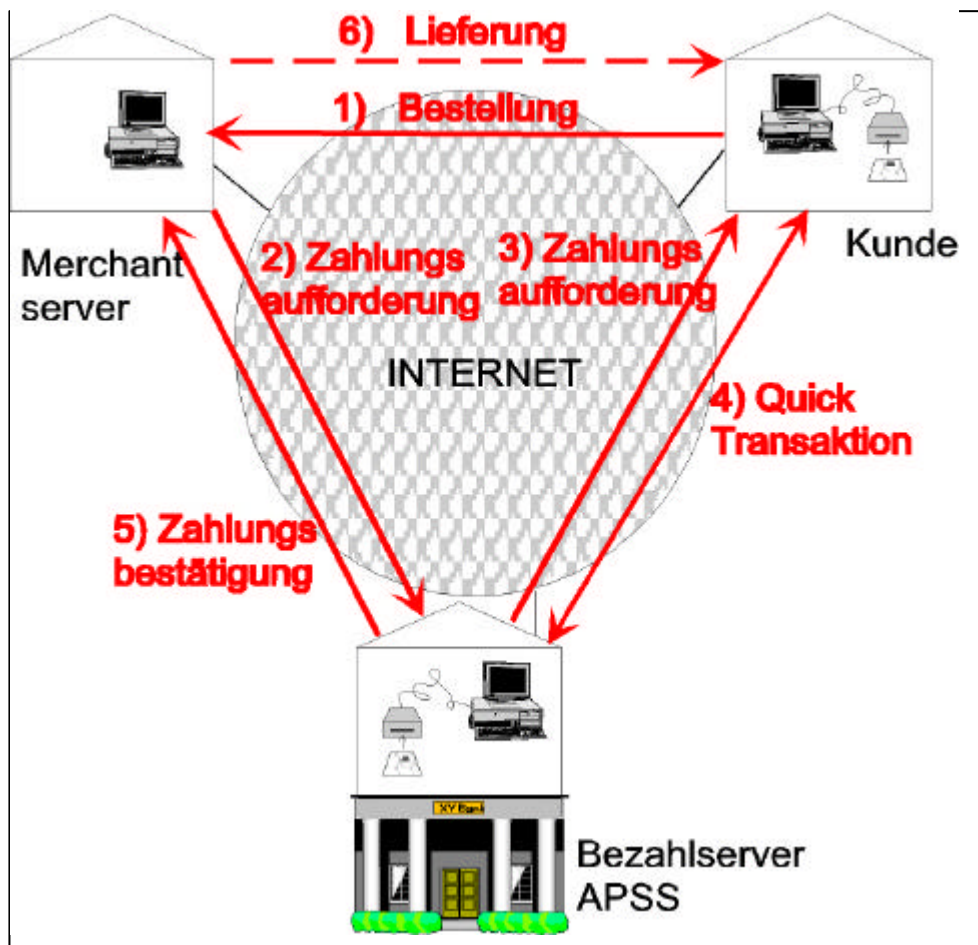


Abb. 1 Infrastruktur Projekt "Quick im Internet"

So funktioniert's:

Der Bezahlvorgang besteht aus folgenden Schritten: Der Kunde sitzt zu Hause vor seinem Browser und stellt sich seinen elektronischen Einkaufskorb zusammen. Wenn er alle Waren ausgewählt hat, die er kaufen möchte, bestätigt er seine Bestellung und schickt diese an den Merchantserver. Der Merchantserver schickt einen Inkassowunsch an den Bezahlserver (auch

Zahlungsaufforderung oder *Payment Request* genannt). Der Bezahlserver stellt über die Client-Software die Verbindung zwischen der Kundenkarte am PC und einer Terminalkarte des betreffenden Händlers am Bezahlserver her. Die Kundenkarte und die Terminalkarte führen dann die Quick-Bezahltransaktion durch. Erfolg oder Mißerfolg dieser Bezahltransaktion meldet der Bezahlserver an den Merchantserver. Daraufhin kann der Merchantserver die Auslieferung der Ware veranlassen.

Mit Korrektur

Falls die Zahlungstransaktion wegen Internet-Kommunikationsproblemen fehlschlägt, wird die Bezahlung natürlich mittels Korrekturtransaktion - entweder gleich anschließend oder bei länger anhaltenden Verbindungsproblemen vor dem nächsten Zahlungsveruch des Kunden - zum erfolgreichen Ende gebracht. Zu diesem Zweck darf aber die Terminalkarte in der Zwischenzeit keine neue Bezahlung entgegennehmen und bleibt sozusagen "gesperrt", bis die Korrekturtransaktion endlich durchgeführt wird (oder die Terminalkarte aus Terminalkartenmangel trotzdem freigegeben werden muß).

Kartenleser – jetzt und zukünftig

Derzeit wird der ChipX der Firma PDTS von der Quick-Clientsoftware unterstützt. Ebenfalls unterstützt wird der Kartenleser, der in mehreren Tastaturen der Firma Cherry eingebaut ist. "Quick im Internet" wird in Zukunft auch die PC/SC-Schnittstelle unterstützen, die durch ein von Microsoft angeführtes Konsortium als allgemeine Smartcard-Leser-Schnittstelle definiert wird. Anpassungen an weitere Kartenleser führt das ICT auf Anfrage durch.

In Zukunft ins Auge zu fassende Erweiterungen, die bereits in das Systemkonzept eingeplant sind, umfassen zum Beispiel einen sogenannten *Secure Cardreader*. Bei diesem ist ein Kryptomodul eingebaut. Weiters ist die Erweiterung des Kartenlesers um eine numerische Tastatur sinnvoll. Dies hat den Vorteil, daß eine allfällige PIN-Eingabe nicht mehr auf dem potentiell infiltrierbaren PC stattfindet und dann an den Kartenleser weitergegeben wird, sondern gleich auf dem sicheren Kartenleser. Außerdem denkbar wäre die Verwendung einer eigenen OK-Taste auf dem Kartenleser, deren Betätigung erst die Bezahltransaktion starten läßt.

Echteinsatz und Zukunft

Dieses System wurde von in enger Kooperation zwischen der EPA/APSS und der TU Wien (Institut für Computertechnik (ICT), o.Univ.-Prof. Dr. Dietmar Dietrich) entwickelt. Das Projekt wurde anfangs von BAWAG und Telekabel finanziert und befindet sich seit Anfang Februar 1998 im Eigentum der EPA/APSS.

Auf der IFABO konnte es - als Pilotversion vorgestellt - bereits große Anerkennung der Experten ernten. Quick im Internet wird nach einem TU-internen Feldversuch, der Mitte Juni durchgeführt wurde, ehebdigst in den Echtbetrieb gehen. Die EPA / APSS nimmt zurzeit noch gerne Pilothändler in das Projekt auf. Interessierte wenden sich bitte direkt an Europay, robert.komatz@europay.at. Als Disagio werden dem Vertragspartner (Händler) 1,5 % vom Umsatz verrechnet.

Zu den Autoren:

DI Norbert Thumb, TU Wien, Institut für Computertechnik

DI Mag. Martin Manninger, TU Wien, Institut für Computertechnik

Robert Komatz, Produktmanager Elektronische Geldbörse, Europay Austria



Veranstaltungen

Konferenzen, Messen

<u>14.-15.9.98</u>	Kartengipfel '98 D-CH-A <i>Smart Card Forum</i> <i>SCFD@compuserve.de</i>	Wien
17.-19.9.98	Cards Australia ,98	Sydney
27.-30.9.98	US: Embedded Systems Conference West	San Jose
<u>30.9.98</u>	ASA Signaturtagung <i>asa@ict.tuwien.ac.at</i>	Wien
27.-29.10.98	Cartes '98 <i>cartes@exposium.fr</i>	Paris
26.-29.11.98	Gute Karten	Wiesbaden
11.98	Cardea 98 Bratislava	SK
11.98	CTST West	USA
13.-15.1.99	OMNICARD <i>inTIMEbln@aol.com</i>	Berlin
23.-25.2.99	Smart Card 99 <i>+44 1895 454534</i>	London
18.-24.3.99	CeBIT 99 <i>www.cebit.de</i>	Hannover
11.-14.5.99	CardTech/SecurTech <i>ctst@ctst.com</i>	Chikago
29.6.-1.7.99	Cards EasternEurope <i>+44 171 827 4154</i>	Warschau

Deutschland - Österreich - Schweiz: Kartengipfel '98

Kontaktlose Karten

Kundenbindung

Zahlungssysteme

Herstellung

14. bis 15. September 1998 im Renaissance Penta Vienna Hotel, Ungargasse 60, A-1030 Wien
Tel: (+43)-1-711 75-0, Fax: (+43)-1-711 75-90
organisiert vom Smart Card Forum Deutschland (SCFD)

In Pilotprojekten in Großstädten ist es bereits möglich: Die Karte ersetzt nicht nur das Bargeld sondern auch den Fahrschein und andere Tickets in den unterschiedlichsten Anwendungsbereichen. Mit der neuen, kontaktlosen Generation der Smart Cards muß die Karte nicht einmal mehr in ein Terminal zum Lesen eingeschoben werden. Kontaktlose Karten sind unübertroffen schnell und witterungsunabhängig. An Skipässen, im ÖPNV, auf Messen oder bei kulturellen und sportlichen Veranstaltungen, überall kann man sie problemlos und zeitsparend einsetzen.

Mit kontaktlosen Karten eröffnen sich neue und faszinierende Perspektiven der jetzt schon vielfältigen Anwendungsmöglichkeiten für Chipkarten. Ob kontaktbehaftet oder kontaktlos, elektronische Geldbörsen-Systeme gibt es bereits in mehreren europäischen Ländern für jede Währung. Wie werden sie miteinander harmonisieren, wenn es die neue europäische Währung gibt?

Wie stellen sich die Hersteller von Karten aber auch von Terminals und Lesegeräten darauf ein? Überhaupt: Welche neuen Herstellungsverfahren, welche neuen Materialien gibt es für Chipkarten?

Diese und weitere Fragen will der Kartengipfel '98 beantworten.

Und schließlich geht es auch um das geradezu klassische Einsatzgebiet von Karten in der Kundenbindung. Mit der Technologie der Chipkarten eröffnen sich neue, individuellere und flexiblere Möglichkeiten. Neue Konzepte zur Kundenbindung, sowie im Bereich des Tourismus und City-Marketing werden vorgestellt.

Nutzen Sie die Chance, erfolgreiche Konzepte und zukunftsweisende Technologien kennenzulernen. Treffen Sie Fachleute und Branchenprofis.

Sichern Sie sich Ihren Platz und melden Sie sich gleich an!

Ausstellungsflächen sind vorhanden!

Wenn Sie Interesse daran haben, Ihr Unternehmen auf dieser Konferenz zu präsentieren und Ihre Produkte auszustellen, wenden Sie sich bitte bis 25. August 1998 an uns

Anmeldeformular

Deutschland - Österreich - Schweiz: Kartengipfel '98

Fax an (+49) 4131-983498

Annette Harraß, Hans Harald Huber,
Lüner Rennbahn 7, D-21339 Lüneburg
Tel. (+49) 4131 - 98 34 14, Fax (+49) 4131 - 98 34 98
SCFD@compuserve.de

Ja, ich nehme am 14. und 15. September an der Konferenz "Deutschland - Österreich - Schweiz: Kartengipfel '98" in Wien teil.

Teilnahmegebühr: 2.790,- DM (zzgl. 16 % MwSt.)

Besonders ermäßigte Gebühr für Mitglieder des ASA: 1.850,- DM (zzgl. 16 % MwSt.)

Wenn meine Anmeldung bis zum 15. August bei Ihnen eingeht, zahle ich eine ermäßigte Teilnahmegebühr in Höhe von 2.390,-DM (zzgl. 16 % MwSt.)

Besonders ermäßigte Gebühr für Mitglieder des ASA: 1.600,- DM (zzgl. 16 % MwSt.)

Ich nehme nur am Montag, 14. September 1998 der Konferenz "Deutschland - Österreich - Schweiz: Kartengipfel '98" in Wien teil.

Teilnahmegebühr: 1.390,- DM (zzgl. 16 % MwSt.)

Besonders ermäßigte Gebühr für Mitglieder des ASA: 950,- DM (zzgl. 16 % MwSt.)

Wenn meine Anmeldung bis zum 15. August bei Ihnen eingeht, zahle ich eine ermäßigte Teilnahmegebühr in Höhe von 1.200,- DM (zzgl. 16 % MwSt.).

Besonders ermäßigte Gebühr für Mitglieder des ASA: 800,- DM (zzgl. 16 % MwSt.)

Ich nehme nur am Dienstag, 15. September 1998 der Konferenz "Deutschland - Österreich - Schweiz: Kartengipfel '98" in Wien teil.

Teilnahmegebühr: 1.390,- DM (zzgl. 16 % MwSt.)

Besonders ermäßigte Gebühr für Mitglieder des ASA: 950,- DM (zzgl. 16 % MwSt.)

Wenn meine Anmeldung bis zum 15. August bei Ihnen eingeht, zahle ich eine ermäßigte Teilnahmegebühr in Höhe von 1.200,- DM (zzgl. 16 % MwSt.).

Besonders ermäßigte Gebühr für Mitglieder des ASA: 800,- DM (zzgl. 16 % MwSt.)

Der zweite Teilnehmer der gleichen Firma erhält eine Ermäßigung der Teilnahmegebühr von DM 200,-.

Hiermit melde ich mich verbindlich an, bitte schicken Sie mir eine Rechnung über die Teilnahmegebühr.

Vorname, Name: _____

Firma, Institution: _____

Straße: _____

PLZ-Ort: _____

Datum, Unterschrift: _____

Ich interessiere mich auch für Fachpublikationen zum Thema Chipkarten:

Bitte schicken Sie mir ein Freixemplar der führenden deutschsprachigen Fachzeitschrift "Card Forum"

Bitte schicken Sie mir ein Freiemplar der internationalen, englischsprachigen Fachzeitschrift "Card Forum International"

ASA Jahrestagung 1998

”Digitale Signatur”

ASA Konferenz '98

30. 9. im Vienna Hilton Hotel

**Digitale Signatur -
Umfeld und Anwendung**

Die rasante Entwicklung des elektronischen Datenverkehrs führt dazu, daß immer mehr Geschäfte und Rechtsakte über elektronische Medien abgewickelt werden. Um rechtliche und technische Sicherheit für diese Transaktionen zu gewährleisten, wird weltweit der Einsatz von digitalen Signaturen empfohlen. Eine ausgereifte Technologie steht dafür zur Verfügung. Für flächendeckende Anwendungen fehlen allerdings noch die notwendigen Voraussetzungen; eine entsprechende Infrastruktur muß geschaffen, bzw. für jedermann zugänglich gemacht werden. Ebenso müssen die rechtlichen Voraussetzungen auf globaler, europäischer und nationaler Ebene harmonisiert werden. Hochrangige Gremien befassen sich mit der Ausarbeitung und Abstimmung entsprechender Rahmenbedingungen.

Top aktuelle Informationen von Experten über den Stand der Technik und das gesamte Umfeld bieten wir Ihnen bei der diesjährigen Konferenz am 30. 9. im Vienna Hilton Hotel.

Programmorschau

<u>Vortragender</u>	<u>Firma</u>	<u>Thema</u>
Hr. Dir. Tischler	OeNB	Moderation
Hr. Prok. Holzbach	STUZZA	Prinzipien, Komponenten
Hr. Mag. Schischka	CZS	digitale Signatur in der Praxis
Hr. Dr. Trcka	EPA / APSS	Projekt der österr. Geldinstitute
Hr. Dr. Brenn	BM Justiz	EU Richtlinie / Gesetz
Hr. Dansachmüller	UTIMACO	kryptographische Grundlage, Anwendung BRD
Hr. Dipl. Math. Keus	BSI	Sicherheit / Zertifizierung
Hr. Min. Rat. Bezdicek	BM Finanzen	der elektronische Amtsweg
Hr. o. Univ.-Prof. Dr. Fuchs	WU-Wien	Globale Perspektiven Signatur und e-Zahlung

TEILNAHMEGEBÜHREN

ASA-Mitglied : öS 2.800,- Nichtmitglieder: öS 3.800,-

Die Gebühren beinhalten die Teilnahme an allen Vorträgen, die Tagungsbroschüre, Kaffee/Tee, Pausengetränke sowie Mittagessen incl. Einem Getränk. Die Teilnahmegebühr bitten wir auf das Konto Nr. 02310763600 der BAWAG, BLZ.: 14000, zu überweisen. Bei Stornierung oder Nichterscheinen werden 30% der Teilnahmegebühr in Rechnung gestellt. Die Anmeldung ist auf eine andere Person kostenlos übertragbar. Bei Nichtmitgliedern gilt bei gleichzeitiger Anmeldung zur ASA die reduzierte Gebühr für ASA-Mitglieder.

VERANSTALTER und AUSKÜNFTE

ASA, Postfach 81, A-1127 Wien, Tel. (0222) 6151 134 750, Fax. (0222) 6151 134 777.

Die österreichische Chipkartenvereinigung ASA (Austrian Smart-Card Association) wurde 1984 gegründet, ist unabhängig und gemeinnützig. Sie gibt eine eigene Mitgliederzeitung heraus, berät Mitglieder, veranstaltet Konferenzen, etc.. Bei kostenpflichtigen Veranstaltungen haben Mitglieder Anspruch auf Ermäßigung. Die Zusammenarbeit mit vergleichbaren Organisationen im Ausland, Herstellern, Anwendern, Universitäten und Normungsinstituten öffnet jedem Mitglied einen einfachen Zugang zu nationalem und internationalem Chipkarten Know-How.

ASA NEWS September 1998

ASA Konferenz 1998

Digitale Signatur

Bitte Zutreffendes
ankreuzen und
einsenden an:

Vienna Hilton Hotel

Antwortkarte:

<input type="checkbox"/>	Anmeldung für ASA Mitglieder Teilnahmegebühr: ATS 2800,--	<hr/> Vorname/Familiename	ASA
		<hr/> Unternehmen	Postfach 81 1127 Wien
<input type="checkbox"/>	Anmeldung für Nichtmitglieder Teilnahmegebühr: ATS 3800,--	<hr/> Straße	
		<hr/> PLZ / Ort	oder per Fax an: 01-6151134777
		<hr/> Tel / Fax	
		<hr/> Datum	Unterschrift

Aufnahmeantrag

in die ASA

Bitte Zutreffendes
ankreuzen und
einsenden an:

<input type="checkbox"/>	Für persönliche Mitglieder, Jahresbeitrag: ATS 200,--	<hr/> Vorname/Familiename	ASA
		<hr/> Unternehmen	Postfach 81 1127 Wien
<input type="checkbox"/>	Für Firmenmitglieder Jahresbeitrag: ATS 900,--	<hr/> Straße	
		<hr/> PLZ / Ort	oder per Fax an: 01-6151134777
<input type="checkbox"/>	Für fördernde Mitglieder Jahresbeitrag: ATS 3.000,--	<hr/> Tel / Fax	
		<hr/> Datum	Unterschrift

Zimmerreservierungen empfehlen wir im Vienna Hilton Hotel

Tel.: +43 1 71700-0