Elektronischer Zahlungsverkehr im Internet : Pilotversuche in der Schweiz und in Deutschland

Autor(en): **Fuchs-Kittowski, Frank / Gabriel, Peter**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **90 (1999)**

Heft 9

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-901930

Elektronischer Zahlungsverkehr im Internet

Pilotversuche in der Schweiz und in Deutschland

Immer mehr Unternehmen bieten ihre Waren und Dienstleistungen im Internet an. 1998 wurden weltweit bereits über 30 Mrd. US-Dollar im Internet umgesetzt. In zehn Jahren sollen nach Prognosen der Gartner Group viele Branchen bereits 30% ihres Umsatzes über den elektronischen Geschäftsverkehr im Internet realisieren. Ein grundlegendes Problem zur kommerziellen Nutzung des Internets ist die derzeit noch fehlende Unterstützung des Zahlungsverkehrs. Während in den letzten Jahren immer neue Zahlungsverfahren entworfen und implementiert wurden, werden derzeit in diversen Pilotprojekten Geschäftsmodelle für einzelne attraktiv erscheinende Zahlungssysteme entwickelt und erprobt. Dieser Beitrag gibt einen Überblick über die momentan in der Schweiz und in Deutschland verfügbaren und praktisch nutzbaren Internet-Zahlungssysteme und diskutiert ihre Einsatzmöglichkeiten.

In der Schweiz verfügen heute etwa 1,2 Mio. Einwohner, das sind rund 22% der Bevölkerung, über einen Internetzugang. (In Deutschland ist die Internetdurchdringung noch geringer: 7,3 Mio. Nutzer bzw. 8,7% der Bevölkerung.) Handel und Dienstleistungsgewerbe stellen sich auf diesen neuen Weg zu ihren Endkunden ein und bieten ihre Waren verstärkt auch über das Internet an. Grosse Aktivitäten zeigen heute vor allem Anbieter aus den Bereichen Computer, Bücher, CD, Textilien und Reisen. Prognosen gehen davon aus, dass zukünftig bis zu 30% aller Handelsumsätze über das Internet abgewickelt werden. Für den Handel eröffnen sich damit grosse Rationalisierungspotentiale: Die Umstellung der Kundeninformation und -beratung auf Internetsysteme verringert die Kosten für Verkaufsflächen und -personal. Die Bestellung über das Internet kann ohne Medienbruch direkt in das Warenwirtschaftssystem übernommen werden.

Die einzige Schwachstelle in diesem Szenario ist derzeit noch der Zahlungsverkehr. Selbst die grossen Online-Shops im Internet wie etwa die Buchhandlung Amazon oder der Computerhändler Dell lassen ihre Kunden heute bevorzugt noch mit nichtelektronischen Verfahren wie Nachnahme oder Überweisung bezahlen.

Eine standardisierte und sichere elektronische Abwicklung der Bezahlung hätte für den Internethandel grosse Vorteile. Für den Händler sinken die Kosten des Zahlungseinzugs, da für die Zahlungsabwicklung nicht mehr das Medium gewechselt werden muss und eine separate Bearbeitung der Zahlung vermieden werden kann. Für den Privatkunden wird es wesentlich einfacher, international Zahlungen zu tätigen.

Adresse der Autoren
Frank Fuchs-Kittowski, Dipl.-Inform., und *Peter Gabriel,* Dipl.-Inform., Fraunhofer-Institut für Software- und Systemtechnik (ISST), Mollstrasse 1, D-10178 Berlin

Einsatzbereiche

Im Internet werden sehr verschiedene Arten von Waren angeboten. Dies sind zum einen physikalische Güter, vor allem CD, Bücher und Computer, sowie Dienstleistungen, heute meistens Reisen, die online bestellt und bezahlt, aber offline geliefert oder erbracht werden. Zum anderen werden über das Internet zunehmend auch elektronische Güter vertrieben, die auch online ausgeliefert werden können. Dazu gehören Software, digitale Ton- und Bilddokumente sowie Informationen aus Wirtschaftsdatenbanken.

Bei physikalischen Gütern wie Büchern oder Computern ist der zu zahlende Betrag relativ hoch und kann mehrere hundert oder tausend Franken betragen. Für elektronische Güter, zum Beispiel eine Information, ist dagegen meist ein erheblich geringerer Betrag zu entrichten. Dies kann zu dem Problem führen, dass die Transaktionskosten für den Bezahlvorgang im Internet den eigentlichen, für die Information zu bezahlenden Betrag übersteigen. Nach dem Verhältnis zwischen Transaktionskosten und Warenwert unterscheidet man die Zahlungsverfahren

- *Macropayment* für die Bezahlung grösserer Beträge
- *Micropayment* vor allem für die Bezahlung von kleinen Beträgen (z.B. für Informationen). Mit Micropayment-Systemen sollen auch kleine Transaktionen wirtschaftlich abgerechnet werden können.

Im Geschäftskundenbereich wird in der Regel ein gewisses Vertrauen zwischen den Geschäftspartnern vorausgesetzt. Bevorzugte Zahlungsverfahren sind, unter anderem wegen der rationelleren Zahlungsabwicklung, die Rechnungsstellung bzw. das Lastschriftverfahren. Gegenwärtig konzentrieren sich die Internet-Zahlungsverfahren deswegen auf das Endkundengeschäft, das von vielen Transaktionen mit vergleichsweise kleinen Beträgen geprägt ist. Hier ist aufgrund des geringeren Vertrauensverhältnisses zwischen Händler und Kunde die sofortige Bezahlung beim Vertragsabschluss üblich.

Sicherheit

Eine der elementaren Anforderungen an ein Internet-Zahlungssystem ist dessen Sicherheit. Dabei werden drei Eigenschaften unterschieden:

• Ein Internet-Zahlungssystem muss ein hohes Mass an Vertraulichkeit der Daten bieten. Das betrifft zum einen den Schutz der Daten bei der Übertragung im Internet vor der unerwünschten Einsicht durch Dritte. Zusätzlich verlangt wird aber häufig auch der Schutz der Kundendaten, die von den beteiligten Händlern und Finanzinstitutionen gesammelt werden. Hier soll vor allem die Anlage von Kunden-

profilen anhand der Zahlungsdaten verhindert werden.

- Ein Internet-Zahlungssystem muss ausserdem die Integrität der übermittelten Daten wahren: Es soll verhindert werden, dass eine Änderung der Daten während der Übertragung oder der Verarbeitung stattfindet.
- Ebenso wichtig ist es, die Authentizität der Daten zu gewährleisten. Es muss sichergestellt werden, dass die Daten, die von einem Teilnehmer des Handels stammen sollen, tatsächlich von diesem Teilnehmer gesendet wurden und nicht von einem Dritten, der eine falsche Identität vorspiegelt.

Öffentliche und private Schlüssel

Um diesen Sicherheitsanforderungen an Internet-Zahlungssysteme zu genügen, werden von allen Internet-Zahlungsverfahren kryptographische Verfahren eingesetzt. Dabei wird auf den Klartext einer Nachricht ein Algorithmus angewendet, der mit Hilfe eines weiteren Parameters (des sogenannten Schlüssels) den verschlüsselten Text der Nachricht berechnet. Bei symmetrischen Verschlüsselungsverfahren wird derselbe Schlüssel zum Verschlüsseln des Klartextes und zum Entschlüsseln des chiffrierten Textes verwendet (Bild 1). Das Hauptproblem der symmetrischen Verschlüsselungsverfahren ist die sichere Übertragung des geheimen Schlüssels selbst, der daher meistens auf einem anderen Weg als der verschlüsselte Text übermittelt werden muss.

Asymmetrische Verschlüsselungsverfahren (Public-Key-Verfahren) setzen ein Schlüsselpaar aus einem öffentlichen Schlüssel und einem geheimen Schlüssel ein [1]. Der Klartext kann entweder

- mit dem öffentlichen Schlüssel verschlüsselt und anschliessend mit dem geheimen Schlüssel wieder zum Klartext entschlüsselt oder
- mit dem geheimen Schlüssel verschlüsselt und anschliessend mit dem öffentlichen Schlüssel wieder zum Klartext entschlüsselt werden (Bild 1).

Öffentlicher und geheimer Schlüssel werden von ihrem Besitzer gemeinsam durch ein mathematisches Verfahren erzeugt. Der öffentliche Schlüssel ist allgemein zugänglich. Er kann dem Kommunikationspartner per elektronischer Post geschickt, im Internet veröffentlicht oder von einer Zertifizierungsstelle (siehe unten) verwaltet werden. Die wesentliche Eigenschaft der asymmetrischen Verschlüsselungsverfahren ist es, dass der geheime Schlüssel nicht aus dem öffentlichen Schlüssel berechnet werden kann.

Ein asymmetrisches Verfahren kann nicht nur eingesetzt werden, um die Vertraulichkeit einer Nachricht zu wahren, sondern auch um die Authentizität und Integrität der Kommunikation zu gewährleisten. Folgendes Beispiel illustriert diese drei Eigenschaften einer verschlüsselten Kommunikation. Eine Person (Alice) möchte einer andern Person (Bob) eine vertrauliche Nachricht schicken. Alice verschlüsselt die Nachricht mit Bobs öffentlichem Schlüssel und schickt Bob den verschlüsselten Text. Nur Bob kann mit seinem Geheimschlüssel aus dem verschlüsselten Text wieder die ursprüngliche Nachricht herstellen. Damit ist die Vertraulichkeit gewahrt. Integrität und Authentizität können wie folgt gewährleistet werden. Alice verschlüsselt die Nachricht mit ihrem geheimen Schlüssel und schickt Bob den verschlüsselten Text. Bob kann den verschlüsselten Text mit dem öffentlichen Schlüssel von Alice zum Klartext entschlüsseln. Ist der entschlüsselte Text lesbar, kann Bob sicher sein, dass die Nachricht von Alice stammt, denn kein Dritter kann Alices Geheimschlüssel kennen. Damit ist die Voraussetzung geschaffen, um die Gültigkeit eines Dokumentes nicht nur durch eine persönliche Unterschrift, sondern auch durch eine auf asymmetrischer Verschlüsselung beruhenden digitalen Signatur zu bestätigen.

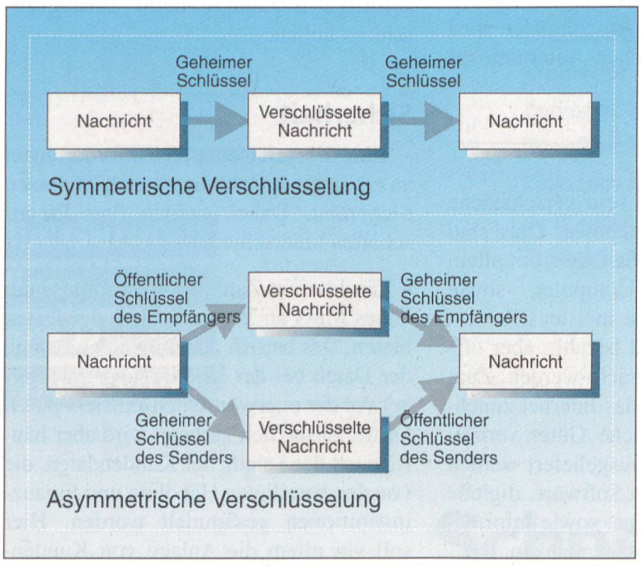


Bild 1 Symmetrische und asymmetrische Verschlüsselungsverfahren

Zertifizierungsstellen

Konkrete Anwendungen der asymmetrischen Verschlüsselungsverfahren beruhen wesentlich auf einem allgemein zugänglichen Katalog, der öffentliche Schlüssel und Besitzer einander zuordnet. Um einen Medienbruch zu vermeiden, sollte dieser Katalog ebenfalls über das Internet angeboten werden. Das naheliegende Verfahren, ein einfaches Verzeichnis der öffentlichen Schlüssel aller Nutzer im Internet zu veröffentlichen, kommt aber nicht in Frage: Es ist unsicher, wie verlässlich ein solches Verzeichnis selbst ist und ob bei der Übermittlung der Verzeichnisinformationen über das Internet nicht Änderungen vorgenommen wurden. Das Verzeichnis der öffentlichen Schlüssel muss also vertrauenswürdig sein und eine sichere Datenübertragung der öffentlichen Schlüssel garantieren. Diese Aufgabe übernehmen Unternehmen oder Behörden, die als Zertifizierungsstellen fungieren. Sie registrieren die Nutzer, verwalten deren öffentliche Schlüssel und stellen sie der Öffentlichkeit zur Verfügung. Alice erhält Bobs öffentlichen Schlüssel von der Zertifizierungsstelle daher in verschlüsselter Form, um die Integrität des Schlüssels zu gewährleisten. Alice entschlüsselt die Nachricht mit dem öffentlichen Schlüssel der Zertifizierungsstelle und kann damit sicher sein, tatsächlich Bobs öffentlichen Schlüssel in den Händen zu halten. Dem öffentlichen Schlüssel der Zertifizierungsstelle kommt daher eine besondere Rolle zu. Er muss jedem Nutzer ohne Fälschungsmöglichkeit übermittelt werden können, zum Beispiel per Diskette oder Voreinstellung in einer speziellen Zahlungssoftware.

In der Schweiz und in Deutschland gibt es mittlerweile mehrere Zertifizierungsstellen. In der Schweiz ist die zurzeit noch einzige Zertifizierungsstelle die Swisskey, eine gemeinsame Tochter von Swisscom sowie der Schweizer und der Liechtensteiner Handelskammer. Deutsche Zertifizierungsstellen sind unter anderem die Daimler-Chrysler-Tochter Debis, der DFN-Verein (Deutsches Forschungsnetz) und die Fraunhofer-Gesellschaft.

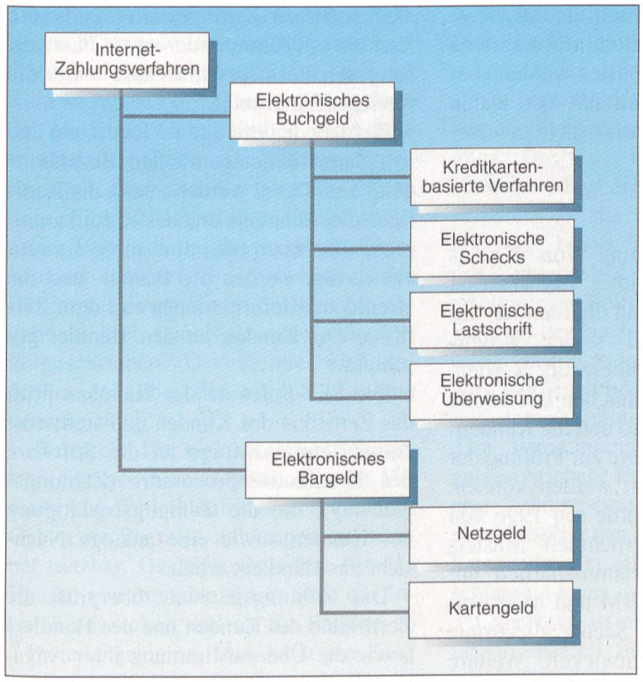


Bild 2 Übersicht über die Internet-Zahlungsverfahren

In Deutschland besteht mit dem Gesetz zur digitalen Signatur seit 1997 eine gesetzliche Regelung für die Einrichtung von staatlich anerkannten Zertifizierungsstellen. Die Regulierungsbehörde für Telekommunikation und Post zertifiziert als oberste deutsche Zertifizierungsstelle andere Zertifizierungsstellen, die dann ihrerseits Nutzerzertifikate ausgeben. Die Telekom hat sich Anfang 1999 als erste deutsche Zertifizierungsstelle gemäss dem Signaturgesetz anerkennen lassen. In der Schweiz wurde bislang auf eine ähnliche Regelung zum deutschen Signaturgesetz verzichtet. Diskutiert wird vor allem, ob die deutsche Regelung für private Zertifizierungsstellen nicht zu restriktiv ist. Auch in den USA geht der Trend eher zu privatrechtlich organisierten Zertifizierungsverbünden.

Zahlungsverfahren und -systeme

Für den traditionellen Versandhandel hat sich in Europa vor allem die Zahlung nach Erhalt der Ware in Form einer Rechnung oder Lastschrift durchgesetzt. Diese bieten den Kunden ein gesetzlich verbrieftes, bedingungsloses Rückgaberecht. Auf diese Weise kann der Kunde die Ware vor der Bezahlung prüfen. Aus der Sicht eines Händlers dagegen werden Vorauszahlung in Form von Vorauskasse und Nachnahme bevorzugt, da in diesem Fall der Händler sicher sein kann, das Geld für seine Leistung zu erhalten. In den USA ist die Bezahlung mit Kreditkarte weit verbreitet. Dabei werden die Kreditkartendaten meist über das Telefon übermittelt. Bei diesem Prinzip erhält der Kunde die Ware erst nach der Zahlungsabwicklung, wobei er aber weitgehende Rechte zur Stornierung der Bestellung besitzt.

Die Internet-Zahlungsverfahren bilden in der Regel existierende Zahlungsverfahren auf das Internet ab. Je nachdem, ob ein Verfahren an ein Bankkonto gebunden ist, unterscheidet man elektronisches Buchgeld und elektronisches Bargeld (Bild 2).

Elektronisches Buchgeld

Elektronisches Buchgeld ist direkt mit einem Konto, zum Beispiel einem Giro- oder Kreditkartenkonto, gekoppelt. Der Betrag wird vom Kundenkonto abgebucht und dem Händlerkonto gutgeschrieben. Heutige Verfahren sind kreditkartenbasierte Verfahren, elektronische Schecks, elektronische Überweisungen und elektronische Lastschriften. Dabei kommt zurzeit der Zahlung mit einer Kreditkarte die grösste Bedeutung zu. Bei kreditkartenbasierten Verfahren werden die Kreditkarteninformationen oder deren Äquivalente über das Internet übertragen. Für den eigentlichen Zahlungsvorgang wird dann die bereits existierende Infrastruktur der Kreditkartenunternehmen genutzt. Je nach dem Zeitpunkt der Verrechnung der Konten von Händler und Kunde (Clearing) und der Verwendung digitaler Zertifikate werden verschiedene Arten der Kreditkartenzahlung unterschieden.

Datenübermittlung via Internet

Vor allem in den USA ist die Übermittlung der Kreditkarteninformationen (Kreditkartennummer, Ablaufdatum, Kundenname) per Telefon, Fax oder Post (Mail Order/Telephone Order [Moto]) und stark zunehmend auch über das Internet verbreitet. Moto-Zahlungen über das Internet verlaufen analog zur Kreditkartenzahlung bei einer Bestellung per Telefon oder Post. Der Kunde trägt seine Kreditkarteninformationen in ein Formular auf einer Internetseite ein, die dann, meistens verschlüsselt, über das Internet zum Händler übertragen werden.

Prüfung und Autorisierung der Kreditkarteninformationen kann der Händler mit einer speziellen Software (z.B. Net-Verify von IC-Verify/Cybercash oder PC Authorize von Tellan Software) online durchführen. Zur Abrechnung werden die Daten offline (in der Regel einmal täglich) an eine Bank weitergeleitet. Die Bank reicht die Transaktionsinformation an einen Kreditkartenprozessor (einen Finanzdienstleister zwischen Händler und Kreditkartenunternehmen, zum Beispiel die Swisspay in der Schweiz oder die Gesellschaft für Zahlungssysteme in Deutschland) weiter, der dann den Zahlungsabschluss durchführt.

Um als Händler Moto-Kreditkartenzahlungen über das Internet anbieten zu können, muss man sowohl einen Vertrag mit einer Handelsbank als auch mit einem Kreditkartenverarbeiter abschliessen. Die Gebühren der Handelsbanken reichen von 1,9 bis 2,7% pro Transaktion, der Kreditkartenverarbeiter berechnet etwa 30 Cent pro Transaktion sowie 10 Dollar pro Monat. Selbst bei einer verschlüsselten Übertragung der Kreditkarteninformationen besteht ein hohes Sicherheitsrisiko, da zum einen der Händler nicht prüfen kann, ob die Daten wirklich vom angegebenen Empfänger stammen, und zum anderen der Kunde nicht sicher sein kann, dass der Händler seine Daten nur für die vorgesehene Transaktion benutzt. Aufgrund dieses höheren Risikos verlangen die Kreditkartengesellschaften bei Moto-Kreditkartenzahlungen und über das Internet übertragenen Kreditkarteninformationen deutlich höhere Provisionen als bei der persönlichen Vorlage der Kreditkarte.

Die Übermittlung der Kreditkarteninformationen über das Internet ist ein technisch einfaches Macropayment-Verfahren und entsprechend oft anzutreffen. Allerdings werden dabei weder die Integrität noch die Authentizität der Kreditkarteninformationen geprüft.

Online-Clearing der Kreditkartenzahlung

Bei der Übermittlung der Kreditkarteninformationen über das Internet er-

folgt die Verrechnung offline. Beim Online-Clearing der Kreditkartenzahlung werden die Verrechnungsinformationen während des Kaufvorgangs an den Kreditkartenprozessor weitergereicht, so dass dem Händler eine höhere Zahlungssicherheit geboten wird. Online-Clearing-Systeme werden von mehreren Firmen angeboten, unter anderem von Swissonline, Globe ID Software, IBM und Cybercash. Über den grössten Marktanteil verfügt das US-Unternehmen Cybercash mit dem gleichnamigen Online-Clearing-System für Kreditkarten.

Cybercash wird in Deutschland von mehreren Banken und Sparkassen wie der Dresdner Bank, der Hypo-Vereinsbank und der West-LB angeboten. In der Schweiz spielt Cybercash keine Rolle.

Händler und Kunden, die Cybercash einsetzen wollen, benötigen ein Cybercash-Verrechnungskonto bei der sogenannten Wallet-Bank, die die Kreditkarte herausgibt. Das Cybercash-System besteht aus drei Softwarekomponenten:

- dem Cybercash-Wallet beim Kunden,
- dem Cybercash-Register beim Händler und
- dem Cybercash-Gateway, das die Kommunikation zwischen dem Händler und dem Kreditkartenprozessor abwickelt. In Deutschland wird das Cybercash-Gateway von der Cybercash GmbH betrieben.

Für den Händler fallen eine einmalige Registrierungsgebühr und transaktionsabhängige Gebühren an, die von Bank zu Bank unterschiedlich sind. Die Kreditkartenzahlung mit Cybercash folgt diesem Ablauf:

- Die Zahlungsdaten, einschliesslich der Kreditkarteninformationen, werden verschlüsselt vom Kunden an den Händler übermittelt.
- Der Händler fügt zu diesen Daten seine eigenen hinzu und überträgt diese an das Cybercash-Gateway.
- Im Cybercash-Gateway werden die Daten abgeglichen bzw. überprüft. Bei erfolgreicher Prüfung führt das Gateway eine Autorisierungsanfrage an den Kreditkartenprozessor durch. Ist die Kreditkarte gültig, erteilt der Kreditkartenprozessor dem Cybercash-Gateway die Freigabe. Vom Gateway erhält der Händler eine Bestätigung über die Autorisierung.
- Darauf erhält der Käufer eine Nachricht vom Händler, dass die Transaktion erfolgreich war.

Das Online-Clearing der Kreditkartenzahlung bringt für den Händler eine höhere Zahlungssicherheit als die Übertragung der Kreditkarteninformationen über das Internet. Ansonsten werden aber Integrität und Authentizität der Daten auch beim Online-Clearing nicht gewährleistet.

SET

Mit der Übertragung von Kreditkarteninformationen über das Internet und mit Cybercash kann die Identität des Kunden nur anhand seiner Kreditkarteninformationen überprüft werden, während bei der persönlichen Bezahlung mit Kreditkarte ein Foto und die Kundenunterschrift auf der Karte zur Prüfung der Identität herangezogen werden können. Aus diesem Grund wurde seit 1996 von den Kreditkartenunternehmen Mastercard und Visa in Zusammenarbeit mit Softwarefirmen wie IBM und Microsoft der Industriestandard Secure Electronic Transaction (SET) entwickelt. Weitere Kreditkartenunternehmen wie American Express und Diners Club sollen in das SET-Konsortium aufgenommen werden. Eine Reihe von Herstellern, unter anderem IBM und Brokat, bietet SET-konforme Zahlungssysteme an.

Der Kunde benötigt je nach Anbieter der SET-Software einen modernen, Javafähigen Internetbrowser oder einen beliebigen Browser mit einer speziellen Software, der SET-Wallet. Ausserdem muss er seine Kreditkarte bei der ausgebenden Bank für die Bezahlung über das Internet freischalten lassen und sich ein Zertifikat besorgen, das im Browser bzw. der SET-fähigen Software mit den beteiligten Schlüsseln installiert wird. Um als Händler SET-Transaktionen abwickeln zu können, muss für die jeweilige Kreditkarte ein Vertrag mit einem Kreditkartenprozessor geschlossen und entsprechende SET-Software in seinen Online-Shops integriert werden.

Bei SET werden Zertifikate zur eindeutigen Identifikation der Teilnehmer (Käufer, Händler) benutzt. Diese Zertifikate stammen von SET-Zertifizierungsstellen. Allerdings besitzen derzeit die wenigsten Händler und Kunden die erforderlichen Zertifikate, und die SET-Zertifizierungsstellen befinden sich teilweise gerade erst im Aufbau. Die Rolle einer Zertifizierungsstelle für die SET-Zertifikate wird beispielsweise in der Schweiz von der Swisskey oder in Deutschland von der Firma TC TrustCenter übernommen.

Eine SET-Transaktion geschieht nach folgendem vereinfachtem Ablauf (Bild 3)

- Der Kunde wählt in seinem Internetbrowser die Bezahlung mit SET aus. Die SET-Software wird gestartet und vom Kunden mit Kennummer sowie Passwort freigeschaltet. Anschliessend wird die Rechnung angezeigt.
- Der Kunde bestätigt die Rechnung und löst damit den eigentlichen Bezahlvorgang aus. Dabei werden zuerst die Zertifikate des Händlers und des Kreditkartenprozessors überprüft. Sind diese vertrauenswürdig, werden die Bestell- und die Kreditkarteninformationen mit dem Zertifikat des Kunden an den Händler geschickt.
- Die SET-Software des Händlers prüft das Zertifikat des Kunden und stellt eine Autorisierungsanfrage an die Software des Kreditkartenprozessors (Zahlungsgateway), die die Zahlungsbestätigung des Kunden sowie eine analoge Nachricht des Händlers erhält.
- Das Zahlungsgateway überprüft die Zertifikate des Kunden und des Händlers sowie die Übereinstimmung ihrer Angaben über die Währung, den Betrag und eventuell andere Angaben. Sind die Prüfungen erfolgreich, werden die Nachrichten an die Kreditkartengesellschaft weitergegeben.
- Durch die Kreditkartengesellschaft wird die Gültigkeit der Kreditkarte des Kunden und das Vorliegen eines Vertrages mit dem Händler geprüft.
- Das Ergebnis wird an das Zahlungsgateway und von dort an den Händler weitergeschickt.
- Ist das Prüfung positiv, wird der Kauf dem Kunden bestätigt.

Da SET ein sehr aufwendiges Zertifizierungsverfahren mit relativ hohen Transaktionskosten darstellt und somit erst für grössere Beträge geeignet ist, erscheinen für kleinere Beträge einfachere Verfahren als ausreichend. Aus diesem Grund wurden Vereinfachungen von SET entwickelt. Dies ist zum einen Merchant-originated SET (Moset), das SET (Zertifikate und Verschlüsselung) nur zwischen Händler und Bank einsetzt und die Kommunikation zwischen Kunde und Händler lediglich verschlüsselt. Zum anderen ist dies SET Certless Modus, bei dem überhaupt keine Zertifikate eingesetzt werden.

Im Gegensatz zu den Moto- und Online-Clearing-Verfahren bietet das Macropayment SET einen sehr hohen Sicherheitsstandard bezüglich Integrität, Authentizität und Datensicherheit.

Elektronische Schecks

Bei Verfahren mit elektronischen Schecks benötigt der Kunde von seiner Hausbank eine Zahlungsautorisierung. Davon erhält ein Kunde, ähnlich den rea-

len Schecks, meist eine grössere Anzahl, um nicht für jede Überweisung eine neue Autorisierung beantragen zu müssen. Zum Bezahlen der gekauften Waren sendet der Kunde dem Händler einen elektronischen Scheck als Zahlungsautorisierung. Der Händler reicht diesen Scheck zur Gutschrift auf sein Konto bei seiner Bank ein, die ihn an die Bank des Kunden weiterleitet. Der entsprechende Betrag wird vom Konto des Kunden abgebucht und dem Konto des Händlers gutgeschrieben. Der Kunde wird anschliessend über die erfolgte Zahlung benachrichtigt.

Beispiele für elektronische Schecks sind Cybercoin von Cybercash oder Minipay von IBM. Allerdings ist derzeit nur Cybercoin für reale Zahlungen im Internet nutzbar. Das System wurde für den Handel von digitalen Waren über das Internet entwickelt und ist für Beträge ab 5 Pfennig geeignet. Man kann pro Kauf maximal 200 DM ausgeben, pro Woche maximal 1000 DM. Diese Beschränkung ist notwendig, da die Banken dem Händler eine Zahlungsgarantie auf Cybercoin-Zahlungen geben. Ein Widerruf der Zahlung ist nicht möglich.

Die Voraussetzungen für den Einsatz von Cybercoin sind dieselben wie bei Cybercash (siehe Abschnitt «Online-Clearing der Kreditkartenzahlung»). Zentrale Bestandteile des Zahlungssystems sind die Schattenbuchhaltung im Cybercash-Zahlungsgateway und das zugehörige Verrechnungskonto bei einer Wallet-Bank.

Für eine Zahlung mittels Cybercash muss zunächst ein ausreichender Betrag auf das Verrechnungskonto geladen werden. Dazu weist der Kunde das Cybercash-Zahlungsgateway an, den gewünschten Betrag von seinem privaten Bankkonto auf seine Cybercash-Geldbörse, die eigentlich durch das Verrechnungskonto dargestellt wird, zu transferieren. Dieser Betrag muss ein Vielfaches von 20 DM sein. Sobald die Echtheits- und die Ursprungsprüfung dieser Anforderung erfolgreich abgeschlossen sind, nimmt das Zahlungsgateway die entsprechende Buchung auf dem Verrechnungskonto vor, indem es im Auftrag der Wallet-Bank eine Lastschrift zu Lasten des Bankkontos des Kunden und zugunsten des Verrechnungskontos der Wallet-Bank erzeugt.

Kauft der Kunde bei einem Internethändler, der Cybercash unterstützt, eine digitale Ware (z.B. ein Programm), so wird diese zunächst zusammen mit einer Cybercoin-Zahlungsanforderung an den Kunden gesendet. Der Kunde bestätigt die Zahlungsanforderung und sendet die Bestätigung zusammen mit allen nötigen Sicherheits- und Identifikationsmerkmalen an den Händler zurück. Da diese Daten verschlüsselt sind, hat der Händler keinen Einblick in die Zahlungsbestätigung. Die Cash-Register-Software des Händlers hängt die Cybercash-Daten des Händlers an die Kundendaten an und überträgt beide Informationsblöcke an das Cybercash-Zahlungsgateway. Nach erfolgreicher Prüfung von Ursprung und Echtheit der Nachricht sowie der Plausibilität der Kunden- und Händlerdaten wird das Verrechnungskonto des Kunden mit dem Zahlungsbetrag belastet und dem Verrechnungskonto des Händlers gutgeschrieben. Der Händler erhält dann eine Zahlungsbestätigung und überträgt abschliessend den Schlüssel, mit dem der Kunde die gekaufte digitale Ware entschlüsseln kann.

Cybercoin ist ein Micropayment-Verfahren speziell für elektronische Güter mit hohen Sicherheitsstandards für die Datensicherheit, insbesondere bezüglich der Anonymität der Kunden. Die Integrität der Daten wird durch das Cybercash-Gateway gewahrt.

Elektronische Lastschriften

Bei einer elektronischen Lastschrift ist nicht der Kunde, sondern der Händler Initiator des Zahlungsvorgangs. Voraussetzung ist eine Einzugsermächtigung des Kunden, die beim Händler vorliegen muss. Die Banken verlangen bisher eine Unterschrift des Kunden für jede Lastschrift. Da dies bei elektronischen Verfahren nicht mit angemessenem Aufwand zu realisieren ist, arbeiten alle Anbieter dieses Verfahrens mit einer elektronischen Buchungskarte, für die der Kunde einmalig einen schriftlichen Einziehungsauftrag erteilt.

Sobald der Kunde Waren beim Händler einkauft, weist der Händler seine Empfängerbank an, das Konto des Kunden bei der Herausgeberbank mit dem fälligen Zahlungsbetrag zu belasten und seinem Händlerkonto gutzuschreiben. Die Bank des Händlers zieht daraufhin den entsprechenden Betrag vom Konto des Kunden bei dessen Bank ein. Bei erfolgter Zahlung erhält der Kunde eine Benachrichtigung über die Abbuchung.

Beispiele für die Umsetzung einer elektronischen Lastschrift sind Electronic Direct Debit (EDD) von Cybercash und das Elektronische Lastschriftverfahren (ELV) von Telecash/Brokat. Ausserdem ist im Rahmen von SET ein elektronisches Lastschriftverfahren in Vorbereitung, das sogenannte SET EDD.

Das elektronische Lastschriftverfahren EDD wurde ebenfalls von der Firma Cybercash entwickelt. Die Voraussetzungen für den Einsatz von EDD sind wiederum dieselben wie bei Cybercash. Wie bei der Kreditkartenzahlung mit Cybercash werden die Zahlungsdaten verschlüsselt an den Händler übermittelt. Der Händler fügt diesen Daten seine eigenen Daten hinzu und überträgt diese an das Cybercash-Gateway. Dieses führt eine Prüfung von Ursprung, Echtheit und Plausibilität der Daten durch. Darauf erhält der Händler eine Bestätigung über den Zahlungsvorgang vom Gateway. Der Händler erstellt dann eine Transaktionsbestätigung für den Kunden und liefert die Ware aus. Das Gateway speichert alle Forderungen des Händlers. Sobald im Cash-Register die Ausgabe der Ware registriert wurde, werden die entsprechenden Datensätze in einem Standardformat an die Bank des Kunden geliefert. Anhand dieser Daten erfolgt die Abwicklung des Lastschriftverfahrens zwischen der Bank des Kunden und der des Händlers.

Elektronische Überweisung

Bei einer elektronischen Überweisung sendet der Kunde seiner Empfängerbank bzw. seinem Finanzdienstleister einen

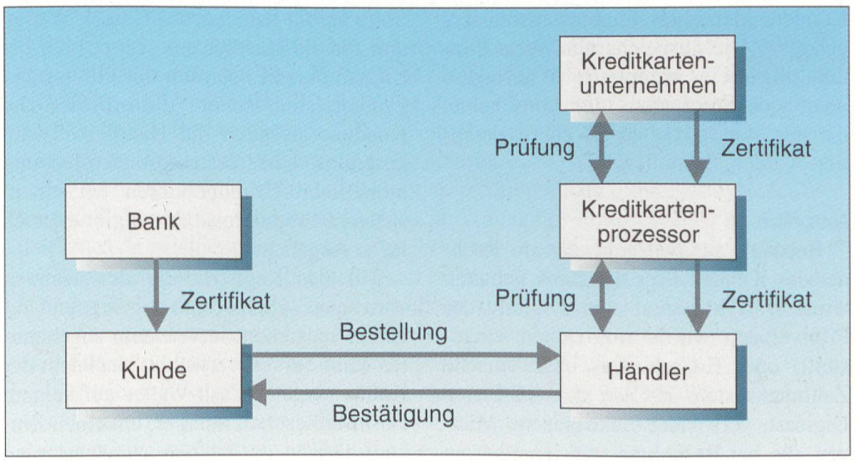


Bild 3 SET-Transaktionen

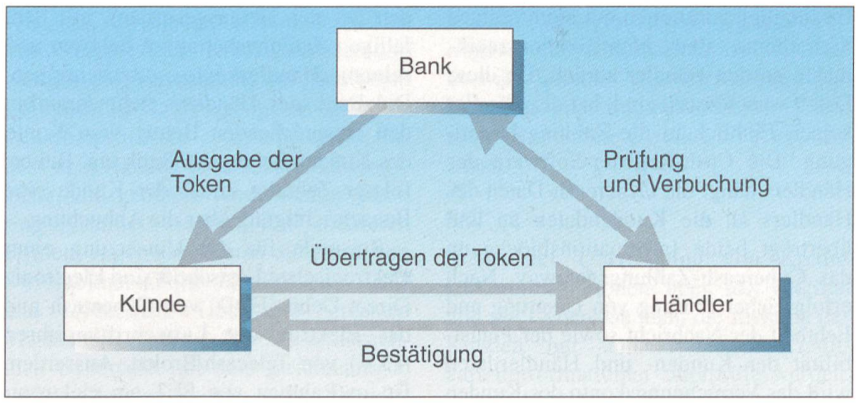


Bild 4 E-Cash-Transaktionen

Überweisungsauftrag von seinem Konto auf das Konto des Händlers. Die Bank überweist den genannten Betrag auf das Konto des Händlers und benachrichtigt ihn daraufhin über die eingegangene Zahlung. Derzeit existieren noch keine praktisch nutzbaren Zahlungssysteme, die nach dem Prinzip der elektronischen Überweisung arbeiten.

Elektronisches Bargeld

Elektronisches Bargeld wird in Form von elektronischen Datensätzen (Token) direkt zwischen Händler und Käufer transferiert. Dabei muss sich der Kunde zunächst Geld in Form von virtuellen Münzen von der Herausgeberbank besorgen. Im Falle einer Zahlung werden die Token zum Händler übermittelt. Der Händler reicht die Token bei seiner Hausbank ein. Diese kontaktiert dann die Herausgeberbank, um die virtuellen Münzen in reales Geld einzutauschen. Elektronisches Bargeld kann nach dem Medium der Speicherung in Netzgeld und Kartengeld unterschieden werden. Kartengeld wird auf elektronischen Karten wie Magnetkarten, Barcodekarten oder meist Chipkarten gespeichert. Über das Netz wird das Geld lediglich übertragen. Netzgeld dagegen wird auf dem Rechner des Kunden oder eines Finanzdienstleisters gehalten. Die gespeicherten Werte können allgemein akzeptierte Währungen oder auch Wertcupons und Gutscheine, die nur von speziellen Händlern akzeptiert werden, darstellen.

Netzgeld

Beispiele für Netzgeld, das im Rechner des Kunden oder der Bank gehalten wird, sind Millicent von Digital (der Pilotversuch wurde inzwischen eingestellt) oder E-Cash. Das elektronische Zahlungssystem E-Cash der US-Firma Digicash verwendet elektronische Münzen, die bei Bezahlung vom Kunden an den Händler geschickt werden. E-Cash ist für Zahlungsbeträge in Grössenordnungen von 10 Rappen bis 400 Franken und somit auch für den Verkauf digitaler Güter über das Internet geeignet.

In der Schweiz führt eine Tochter der Credit Suisse, die Swiss Netpay, einen E-Cash-Pilotversuch durch. Derzeit sind in der Schweiz 28 Händler aus unterschiedlichen Branchen und 3000 Kunden beteiligt. In Deutschland ist es die Deutsche Bank, die das System sowohl Kunden als auch Händlern in einem Pilotprojekt zur Verfügung stellt. Momentan kann man in Deutschland mit E-Cash bei 28 Händlern einkaufen. Die Anzahl der Kunden beträgt über 3200.

Ein deutlicher Vorteil des Schweizer gegenüber dem deutschen Pilotprojekt ist, dass es für die Teilnahme ausreicht, ein Konto bei irgendeiner Schweizer Bank zu haben. Beim deutschen Projekt ist die Voraussetzung für den Einsatz von E-Cash – sowohl für Händler als auch für den Kunden – ein Bankkonto bei der Deutschen Bank. Im Gegensatz zur Deutschen Bank arbeitet die Swiss Netpay daran, dass sich bald auch andere Banken am Pilotversuch beteiligen.

Ein E-Cash-Konto kann der Kunde bei der entsprechenden Bank online beantragen. Diese gibt auch die erforderliche Software für Kunden, das E-Cash-Wallet, und für die Händler aus. Da es sich bei E-Cash derzeit noch um ein Pilotprojekt handelt, sind sowohl die erforderliche Kunden- als auch die Händlersoftware kostenlos. Über Transaktionskosten und monatliche Grundgebühren bei einem späteren Produktionsbetrieb gibt es noch keine Angaben.

Mit der Registrierung des Kunden wird sein E-Cash-Konto angelegt und auf einem speziellen Server, dem sogenannten Mint-Server, verwaltet. Nachdem der Kunde seine E-Cash-Wallet auf seinem PC installiert hat, muss er, um einen Einkauf tätigen zu können, zunächst eine Überweisung auf das E-Cash-Konto vornehmen. Erlaubt sind beim Schweizer Pilotversuch maximal 5000 Franken pro Monat. Von diesem Depot können dann elektronische Münzen in die E-Cash-Geldbörse geladen werden, insgesamt ebenfalls maximal 5000 Franken. Eine Transaktion mit E-Cash hat folgenden Verlauf (Bild 4):

- Möchte der Kunde ein Produkt bezahlen, sendet er an den Server des Händlers den Wunsch, mit E-Cash zu bezahlen.
- Der Händler-Server prüft zuerst, ob der Kunde eine E-Cash-Geldbörse installiert hat. Ist dies der Fall, sendet der Server eine Zahlungsaufforderung an den Kunden bzw. an dessen E-Cash-Wallet.
- Wenn dieser die Zahlungsaufforderung akzeptiert, wird von der E-Cash-Wallet die benötigte Anzahl Münzen an den Händler transferiert. Sind nicht ausreichend Münzen im E-Cash-Wallet vorhanden, hat der Kunde die Möglichkeit, weitere Münzen von seinem E-Cash-Konto in seine Wallet zu transferieren.
- Bei erfolgter Übertragung der Münzen leitet der Händler-Server sie zuerst weiter an den Mint-Server, der die Münzen auf Echtheit und Einmaligkeit überprüft. Letzteres dient dazu, das sogenannte Double Spending, das mehrmalige Verwenden einer Münze, zu verhindern.
- War auch diese Prüfung erfolgreich, werden die Münzen dem E-Cash-Konto des Händlers gutgeschrieben und der Händler benachrichtigt, dass er die bestellte Ware an den Kunden schicken kann, entweder auf konventionellem Weg oder bei digitalen Daten direkt per Internet.
- Der Händler kann sich später den auf seinem E-Cash-Konto angesammelten Betrag seinem realen Bankkonto gutschreiben lassen.

Eine besondere Eigenschaft des Micropayment-Systems E-Cash besteht darin, dass durch den Einsatz von sogenannten blinden Signaturen (Zertifikate, die die Bank für eine virtuelle E-Cash-Münze vergibt, ohne die Seriennummer zu kennen) die Anonymität des Kunden gegenüber Dritten, besonders jedoch gegenüber der herausgebenden Bank gewährleistet wird.

Kartengeld

Eine Geldkarte, wie sie von Banken und Sparkassen angeboten wird, ist eine spezielle Variante des elektronischen Bargelds, bei der das Geld nicht auf dem Rechner des Kunden oder dem Server einer Bank, sondern im Chip der Geldkarte gespeichert wird. Beispiele für Kartengeld sind elektronische Geldbörsen wie die Schweizer Cash-Card, die deut-

sche ZKA-Geldkarte oder das britische Mondex-System.

Die Geldkarten scheinen ein geeignetes Zahlungsmittel für das Internet zu sein, da sie zum einen bereits eine grosse Verbreitung haben und zum anderen auch für kleinere Beträge geeignet sind. Sie setzen allerdings ein spezielles Kartenlesegerät am PC des Kunden voraus.

Erste einsatzfähige Lösungen für Zahlungen mit der Geldkarte im Internet existieren bereits von verschiedenen Anbietern, zum Beispiel Brokat, Telecash, ECRC, Atos. Allerdings sind diese Verfahren in Deutschland noch nicht vom Zentralen Kreditausschuss (ZKA) genehmigt. Der ZKA hat vielmehr Ende Juni 1998 allgemeine Anforderungen an die beim Endkunden einzusetzende Hardware und Software für Zahlungen mit der Geldkarte im Internet formuliert, die Grundlage für die Zulassung solcher Anwendungen sein werden. Es geht dabei insbesondere

- um die Nichtverfälschbarkeit des vom Kunden bestätigten Zahlungsbetrags
- um die Authentizität der Beziehung zwischen Kunde und Händler bzw. Händler und Händlerkarte
- um eine ausreichend sichere und vor Fälschungen geschützte Protokollierung der Zahlungsvorgänge

Ausserdem sollen nur Kartenleser mit integriertem Display für eine Geldkarten-Internet-Lösung in Frage kommen. Dies erhöht die Kosten für den Chipkartenleser von etwa 30–50 DM auf vermutlich 100–150 DM und mehr. Auf Grundlage dieser allgemein formulierten Sicherheitsanforderungen wird momentan eine technische Spezifikation entwickelt, die dann Grundlage für das jeweils notwendige Sicherheitsgutachten für Systemlösungen sein wird.

Ausblick

In den vergangenen Jahren sind eine Vielzahl proprietärer, geschlossener Systeme für den Internet-Zahlungsverkehr entstanden, die nicht miteinander interoperieren können. Dies bringt den Nachteil mit sich, dass zum einen der Wechsel von Geld zwischen diesen Systemen nicht möglich oder sehr aufwendig ist und zum anderen sowohl Händler als auch Kunden mehrere Systeme betreiben müssen, was für beide Seiten aufgrund des erforderlichen Aufwandes nicht akzeptabel ist.

Es ist abzusehen, dass nur wenige Systeme die nötige Marktdurchdringung und Nutzerakzeptanz erreichen werden. Eine Homogenisierung, die alle Händler und Kunden dasselbe System benutzen liesse, würde zwar Interoperationsprobleme vermeiden und die Transaktionen günstiger machen. Allerdings könnte ein solches uniformes System nicht an die individuellen Anforderungen der Kunden und Händler angepasst werden. Insbesondere wären keine Unterscheidungen möglich zwischen

- Micropayment oder Macropayment in Abhängigkeit der Höhe der Transaktionskosten
- dem Handel mit physischen oder digitalen Gütern
- dem Handel mit unterschiedlichen Anforderungen an die Datensicherheit
- der Art der Bezahlung: Vorkasse oder Nachnahme

Erforderlich sind vielmehr Systeme, die zum einen für spezifische Kundenanforderungen offen und anpassbar sind und zum anderen für eine breite Akzeptanz standardisiert sind. Einige Unternehmen bieten bereits Plattformen für verschiedene Zahlungssysteme (z.B. X-Pay von Brokat) an. Darin lassen sich verschiedene Zahlungsverfahren, wie Lastschrift, Kreditkartenzahlung, Geldkarte, integrieren. In Zukunft werden sich voraussichtlich offene, auf Standards basierende Systeme durchsetzen. Ein solcher Standard, wie er mit SET für die Kreditkartenzahlung bereits vorliegt, muss aber erst noch für die gesamte Bandbreite der Internet-Zahlungsverfahren geschaffen werden.

Digitale Signaturen werden, über ihren Einsatz im Zahlungsverkehr hinaus, eine zunehmende Rolle im elektronischen Geschäftsverkehr spielen. Hierfür entsteht gerade eine entsprechende Zertifizierungsinfrastruktur. Offen ist derzeit noch, ob eine eher privatwirtschaftlich orientierte Struktur wie in den USA entsteht oder der Staat regulierend eingreift, wie es in Deutschland mit dem Signaturgesetz vorbereitet wurde. Die digitale Unterschrift hat zurzeit weder in Europa noch in den USA denselben rechtsverbindlichen Charakter wie die eigenhändige Unterschrift. Die Gültigkeit von Verträgen, die mit digitaler Signatur abgeschlossen wurden, ist umstritten, vor allem dann, wenn eine eigenhändige Unterschrift des Vertrags zwingend vorgeschrieben ist. Hier besteht Bedarf nach einer gesetzlichen Regelung.

Literatur

[1] *L. O'Connor:* Sichere Kommunikation im Internet. Bulletin SEV/VSE 89(1998)19, S. 13–19.

[2] *A. Brüggemann-Klein, A. Endres, E. Jessen, R. Weber, H. Werner:* Abrechnungs- und Zahlungskonzepte für Dienstleistungen digitaler Bibliotheken. Informatik – Forschung und Entwicklung 13(1998)3, S. 169–172.

[3] *S. Lukas:* Cyber Money, Künstliches Geld in Internet und Elektronischen Geldbörsen. Neuwied: Luchterhand 1997.

[4] *G. Pernul, A. Röhm:* Neuer Markt – neues Geld? Wirtschaftsinformatik 4(1997), S. 345–355.

[5] *R. Schuster, J. Färber, M. Eberl:* Digital Cash. Zahlungssysteme im Internet. Berlin: Springer 1997.

[6] *M. Stolpmann:* Elektronisches Geld im Internet. Grundlagen, Konzepte, Perspektiven. Köln: O'Reilly 1997.

[7] *P.A. Strassmann:* Overview of Strategic Aspects of Information Management. Technology and People (1982)1.

[8] *R. Weber:* Market Analysis of Digital Payment Systems. Technischer Bericht, Institut für Informatik, TU München 1998 (http://chablis.informatik.tu-muenchen.de).

Les virements électroniques par internet

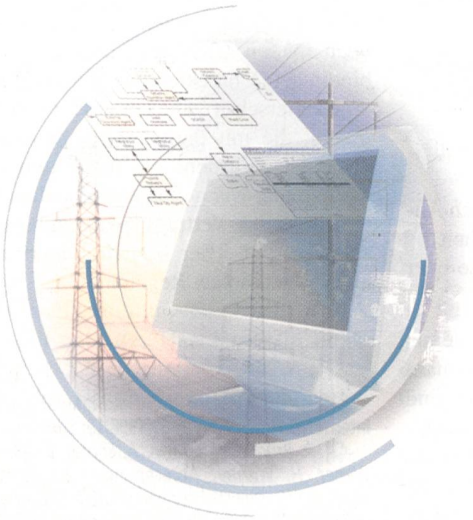
Essais pilotes en Suisse et en Allemagne

De plus en plus nombreuses sont les entreprises qui offrent leurs marchandises et leurs services sur internet. En 1998, le chiffre d'affaires mondial sur internet a été de plus de 30 milliards de dollars. Selon les pronostics du Gartner Group, d'ici dix ans, de nombreuses branches réaliseront plus de 30% de leur chiffre d'affaires par service de paiement électronique sur internet.

Un problème fondamental de l'exploitation commerciale d'internet est jusqu'à présent l'absence de support du service de virements. Tandis que de nouvelles méthodes de paiement ont été développées et mises en œuvre à plusieurs reprises ces dernières années, on est actuellement en train de développer et de tester, dans le cadre de divers projets pilotes, des modèles commerciaux de systèmes de paiement qui semblent intéressants. Ce sont surtout les banques et les entreprises de cartes de crédit qui jouent ici un rôle important.

L'article ci-dessus donne un aperçu des systèmes de paiement sur internet actuellement disponibles et utilisables sur le plan pratique en Suisse et en Allemagne et en examine les possibilités d'utilisation.

TELEGYR® Systeme, die bessere Lösung für Ihr Netzmanagement in konventionellen und deregulierten Energiemärkten.



TELEGYR®, Ihre komplette Lösung für die Verteilnetzführung, die Erzeugung und den Transport von
elektrischer Energie.

Ihre Vorteile:

- Schnelles und effizientes Störungs-Management
- Effizienter Energieeinsatz und sichere Versorgung
- Kosteneffektive Datenerfassung und Datenpflege
- Lastvorhersage und Lastoptimierung
- Zukunftsorientierte Funktionen für das Bestehen im deregulierten Energiemarkt

Telegyr Systems AG
Gartenstadtstr. 2a
CH-6301 Zug
Tel. (+41) 41 724 44 00
Fax (+41) 41 724 44 45
http://www.telegyr.com

Telegyr Systems AG
Mitteldorfstr. 37/39
CH-5033 Buchs
Tel. (+41) 62 832 20 00
Fax (+41) 62 832 20 01

Telegyr Systems SA
ch. des Délices 9
CH-1006 Lausanne
Tel. (+41) 21 613 27 00
Fax (+41) 21 617 57 75

TELEGYR®
SYSTEMS

Für Sie machen wir uns stark!

Mit Rockwell Automation steht Ihnen ein starker Partner zur Seite

Seit mehr als zehn Jahren vereint Rockwell Automation führende Marken der industriellen Automation. Dank dieser Integration eröffnet sich Ihnen ein umfassendes Leistungs- und Produktespektrum – von Antriebstechnik über Motorstarter bis zu Systemlösungen.

Hinter Rockwell Automation steht die Stärke und die Erfahrung eines führenden Hochtechnologie-Unternehmens, das über nachhaltige Ressourcen verfügt.

Bitte verlangen Sie Unterlagen

Rockwell Automation AG
Gewerbepark, 5506 Mägenwil
Tel. 062 889 77 77
Fax 062 889 77 11

Rockwell Automation
Bringing Together Leading Brands in Industrial Automation