LEHRSTUHL FÜR
ALLG. BWL UND WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. HERBERT KARGL

Schwickert, Axel C.; Franke, Thomas

Electronic-Payment-Systeme im Internet

ARBEITSPAPIERE WI
Nr. 8/1996

Schriftleitung:
Dr. rer. pol. Axel C. Schwickert

Information

Reihe: Arbeitspapiere WI

Herausgeber: Univ.-Prof. Dr. Axel C. Schwickert
Professur für BWL und Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Bis Ende des Jahres 2000 lag die Herausgeberschaft bei:

Lehrstuhl für Allg. BWL und Wirtschaftsinformatik
Johannes Gutenberg-Universität Mainz
Fachbereich Rechts- und Wirtschaftswissenschaften
Welderweg 9
D - 55099 Mainz

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IuK-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstanden aus Forschungsarbeiten, Diplom-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen des Lehrstuhls für Allg. Betriebswirtschaftslehre und Wirtschaftsinformatik Univ. Prof. Dr. Herbert Kargl an der Johannes Gutenberg-Universität Mainz.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.
Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber (Gießen) unter obiger Adresse Kontakt auf.
Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe und deren Bezug erhalten Sie auf dem Schlußblatt eines jeden Arbeitspapiers und auf der Web Site des Lehrstuhls unter der Adresse http://wi.uni-giessen.de

Arbeitspapiere WI Nr. 8/1996

Autoren: Schwickert, Axel C.; Franke, Thomas

Titel: Electronic-Payment-Systeme im Internet

Zitation: Schwickert, Axel C.; Franke, Thomas: Electronic-Payment-Systeme im Internet, in: Arbeitspapiere WI, Nr. 8/1996, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1996.

Kurzfassung: Moderne Unternehmen erkennen zunehmend die Chancen eines neuen globalen Marktes im Internet. Ein begrenztes Angebot von käuflich zu erwerbenden Informationen, Gütern und Dienstleistungen existiert bereits heute im Netz. Die weitere Kommerzialisierung wird allerdings durch den Mangel an sicheren Zahlungssystemen gebremst. Sollen die enormen wirtschaftlichen Potentiale des Internet genutzt werden, wird ein System zur sicheren, einfachen und preiswerten Bezahlung per Mausklick erforderlich. Unternehmen, die im Offline-Alltag Ihre Produkte anbieten, werden dies erst dann auch im Internet tun, wenn Sie durch die Möglichkeit der sicheren Abrechnung einen Anreiz dazu erhalten. Analog zum herkömmlichen Zahlungssystem mit z. B. der physischen Übergabe von Bargeld wird ein Internet-Electronic-Payment-System (EPS) ein Zahlungsmittel (elektronisches Geld) und Methoden der Zahlung (elektronische Übergabe) zur Verfügung stellen müssen. Zunächst sind die EPS-spezifischen Anforderungen an diese beiden Komponenten darzulegen, bevor die Realisierungsmodelle (Kreditkarten-Systeme, Debit-/Credit-Systeme, elektronische Währungssysteme) für Internet-EPS skizziert werden.

Schlüsselwörter: Electronic Payment Systems, Transaktionssicherheit, Kryptographie, Datenverschlüsselung, Protokollverschlüsselung, PGP, SSL/ Netscape, S-HTTP, Kreditkarten-Systeme, Debit-/Credit-Systeme, elektronische Währungssysteme, Cybercash, First Virtual, Netbill, NetChex, Digicash, eCash, NetCash, Smartcard-Systeme

Inhaltsverzeichnis

1 Das Internet als globaler Marktplatz

Das Internet entstand aus dem im Jahr 1969 gebildeten ARPAnet (Advanced Research Project Agency, ein experimentelles militärisches Netz) auf der Grundlage eines Vorläufers von TCP/IP, das durch Xerox in den USA entwickelt wurde. Das Internet ist kein geschlossenes Netz, sondern eine Menge von Computern, die alle das Kommunikationsprotokoll TCP/IP verwenden und über Datenleitungen miteinander verbunden sind.[1]

Um Daten an einen entfernten Rechner zu schicken, teilt TCP/IP diese in unabhängige Pakete auf, die über dynamisches Routing zum Empfänger gelenkt werden. Vor der Übertragung ist demnach unbekannt, welche Wege die einzelnen Pakete nehmen und welche Knotenpunkte sie dabei passieren werden.[2] Die unverschlüsselten Daten können theoretisch an jedem Knotenpunkt eingesehen, aufgezeichnet, verändert, ergänzt oder vernichtet werden.

Es war nicht das primäre Ziel der Internet-Konstrukteure, ein Netz mit hohen Übertragungsraten oder der Sicherheit vor kriminellen Netzteilnehmern zu entwickeln, sondern vielmehr die Realisierung eines stabilen, sich quasi selbst reparierenden Rechnerverbundes, der auch nach einem militärischen Schlag noch funktionieren sollte.[3]

Mit der Einführung des World Wide Web geht seit Anfang der 90er Jahre ein stetig wachsender Zulauf zum Internet einher. Durch die einfache graphische Bedienung wandelt sich das einst geschlossene Netz der Forscher zu einem Tummelplatz der breiten Massen. Nach aktuellen Schätzungen sind heute bereits mehr als 40 Mio. Menschen weltweit an das Internet angeschlossen.[4]

Da TCP/IP keine sichere Basis für die unverschlüsselte Übertragung sensibler Daten darstellt, ist das Internet heute mehr ein Werbe- als ein Verkaufsmedium. Wird Handel getätigt, erfolgt die Bezahlung meist über Kreditkarte, indem der Käufer dem Händler die notwendigen Kreditkarteninformationen (Name, Nummer und Gültigkeitsdatum) über das Netz schickt; der Händler fordert daraufhin sein Geld von dem Kreditkartenunternehmen ein. Schickt der Käufer seine Kreditkarten-Daten ungeschützt über das offene Internet, kann ein Angreifer (attacker) diese während der Übertragung mithören (eavesdropping). Er kann Teile der Daten wie beispielsweise die Lieferadresse oder den Geldbetrag ändern (message tampering) oder durch Übermittlung einer falschen IP-Nummer und falschem Usernamen (masquerading techniques) sich unter anderer Identität in Systemen anmelden und z. B. bei einer Bank im Namen des echten Kontobesitzers elektronisches Geld abheben. Die herkömmliche Kreditkartenzahlung wird zwar nicht kategorial, aber graduell signifikant sicherer, wenn der Käufer den Umweg über das Telefon bzw. Fax zur Übermittlung seiner Kreditkarteninformationen nimmt.[5]

---

1 Vgl. Schneider, Gerhard: Eine Einführung in das Internet, in : Informatik Spektrum, 18/95, S. 263.

2 Vgl. Reif, Holger: Netz ohne Angst, in: c't, 9/1995, S. 174.

3 Vgl. Rensmann, Jörg: Strukturchaos Internet, in: N&C, 12/1995, S. 56.

4 Vgl. Schneider, Gerhard: Eine Einführung in das Internet, a.a.O., S. 263.

5 Vgl. Borchers, Detlef: Abrechnungs- und Zahlungsmodalitäten im Internet - ein Überblick, Online im Internet: URL: http://www.ix.de/gw/gw9-95/internet/ecash.html [Stand 1.3.96].

Moderne Unternehmen erkennen zunehmend die Chancen eines neuen globalen Marktes. Ein begrenztes Angebot von käuflich zu erwerbenden Informationen, Gütern und Dienstleistungen existiert bereits heute im Netz. Die weitere Kommerzialisierung wird allerdings durch den Mangel an sicheren Zahlungssystemen gebremst. Sollen die enormen wirtschaftlichen Potentiale des Internet genutzt werden, wird ein System zur sicheren, einfachen und preiswerten Bezahlung per Mausklick erforderlich. Unternehmen, die im Offline-Alltag Ihre Produkte anbieten, werden dies erst dann auch im Internet tun, wenn sie durch die Möglichkeit der sicheren Abrechnung einen Anreiz dazu erhalten.[6]

Damit sich im Internet ein elektronischer Marktplatz entwickeln kann, müssen bestimmte rechtliche Bedingungen erfüllt sein. Eine Markttransaktion benötigt neben den zwei Tauschpartnern, dem Tauschgegenstand und der Bezahlung eine Willenserklärung. Die Willenserklärung muß vor dem Austausch der Waren und der Bezahlung zustande kommen und später rechtlich bewiesen werden können. Dies ist bei Verträgen im Internet problematisch. Da sich die Tauschpartner nicht gegenüberstehen, können sie sich weder gegenseitig identifizieren noch einen konventionellen Vertrag abschließen. Den Vertrag über ein externes Medium, z. B. dem Briefweg, zu erstellen macht meist wenig Sinn, da durch die zeitliche Verzögerung in vielen Fällen die Spontaneität des Mediums Internet nicht mehr zum Tragen kommt. Damit ein verbindlicher Vertrag zustande kommen kann, wird eine Anerkennung digitaler Dokumente erforderlich, die sich durch sogenannte digital signatures und digital notarizations bei angepaßter Rechtsprechung erreichen ließe.[7] Auf die rechtlichen Sachverhalte sei an dieser Stelle der Vollständigkeit halber hingewiesen, da sie in engem Zusammenhang mit Electronic Payment Systems stehen. Von diesen juristischen Problemstellungen wird nachfolgend jedoch abgesehen und nur die Konzeptionen von Zahlungssystemen für das Internet (Internet-Electronic-Payment-System, Internet-EPS, EPS) analysiert.

Analog zum herkömmlichen Zahlungssystem mit z. B. der physischen Übergabe von Bargeld wird ein Internet-EPS ein **Zahlungsmittel (elektronisches Geld)** und **Methoden der Zahlung (elektronische Übergabe)** zur Verfügung stellen müssen. In Kapitel 2 werden zunächst die EPS-spezifischen Anforderungen an diese beiden Komponenten dargelegt, bevor in Kapitel 3 drei verschiedene Realisierungsmodelle für Internet-EPS skizziert werden.

2 Anforderungen an Electronic-Payment-Systeme

2.1 Anforderungen an ein Internet-Zahlungsmittel

Die spezifischen Anforderungen an ein Internet-Zahlungsmittel können aus den Anforderungen an reales Geld abgeleitet und wie folgt gruppiert werden:

6 Vgl. o.V.: Survey on Internet Money, Online im Internet: URL: http://graph.ms.ic.ac.uk/abalysis [Stand 2.3.96].

7 Vgl. Fox, Dirk: Automatische Autogramme, Online im Internet: URL: http://www01.ix.de/artikel/ct9510/Retorte.htm [Stand 9.2.96].

Erfüllung der Tauschmittelfunktion

In erster Linie wird ein Internet-Zahlungsmittel die **Tauschmittelfunktion** zu erfüllen haben. Wie die Anforderungen an das Zahlungsmittel diesbezüglich genau aussehen, ist abhängig von den angebotenen Gütern und Dienstleistungen. Dies werden zum einen nicht-körperliche Leistungen und Informationen sein, wobei das Angebot von Recherchedatenbanken, Lexika und Software über sehr aktuelle Informationen, wie z. B. Börsenticker, bis zu Informations-Dienstleistungen, wie beispielsweise die Berechnung von Fahrtstrecken für Speditionen oder Produkt-Support, reichen wird. Zum anderen werden Produzenten und Händler „hard goods“ elektronisch anbieten und gegen ein Internet-Zahlungsmittel absetzen wollen. Für alle Güter und Dienstleistungen muß die gesamte Bandbreite von Pfennig- (Micropayments) bis zu größeren Beträgen abgedeckt sein und das Zahlungsmittel muß eine allgemeine Akzeptanz bei Käufern und Verkäufern genießen.

Konvertibilität in nationale Währungen

Da es Anbietern und Nachfragern im Internet möglich ist, ortsunabhängig zu agieren sollte das Internet-Zahlungsmittel weltweit akzeptiert werden und über alle Landesgrenzen hinweg in reales Geld nationaler Währungen umgetauscht werden können.

Schutz vor Mißbrauch, Verlust, Diebstahl, Fälschung, Mehrfachverwendung

Das Bezahlen im Internet sollte mindestens so sicher sein wie das Zahlen mit Scheinen und Münzen im „offline-Leben“, wo sich Käufer und Verkäufer unmittelbar gegenüberstehen. Das Beschreiten des Rechtsweges über Landesgrenzen hinaus wird sich als äußerst kompliziert erweisen. Darüber hinaus können Überlegungen einfließen, ob und wie elektronisches Geld einen zusätzlichen Schutz vor Verlust oder Diebstahl im Vergleich zu realem Geld leisten kann. Hierzu zählt auch, daß elektronisches Geld die Anforderungen an die langfristige Wertspeicherfunktion und die Fälschungssicherheit herkömmlichen körperlichen Geldes erfüllt. Ein spezifisches Problem des elektronischen Geldes zeigt sich bei einer möglichen Mehrfachverwendung aufgrund einer fehlenden Körperlichkeit. Elektronische Geldeinheiten sind lediglich Daten, die kopiert werden können. Eine zeitparallele Verwendung kopierter Geldeinheiten ist zu unterbinden.

Interpersonelle Übertragbarkeit

Das Internet-Zahlungsmittel sollte eine „Two Way Function“ besitzen, die es ermöglicht, daß ein Käufer auch Zahlungen anderer Wirtschaftssubjekte entgegennehmen und für eigene Käufe weiterverwenden kann. Die Two Way Function sollte ohne Autorisierung durch Dritte möglich sein.

Offline-Fähigkeit

Elektronisches Geld muß Geschäfte ermöglichen, ohne online im Internet zu sein. Vorstellbar ist hier der Zahlungsmittelaustausch über digitalisierte Offline-Brieftaschen mit isolierter Punkt-zu-Punkt-Verbindung.

Anonymität

Das Zahlungsmittel sollte dem Käufer die gleiche **Anonymität** bieten wie es herkömmliches Geld auch tut. Das heißt, daß ein Händler oder ein Zahlungsmittel-

aussteller idealerweise nicht mit vertretbarem Aufwand zurückverfolgen kann, wer das Zahlungsmittel bereits besessen hat und welche Waren von wem wann damit gekauft wurden.[8] Ist diese Anonymität nicht gegeben, können durch Auswertung von Transaktionsdaten z. B. die Kaufgewohnheiten jedes Teilnehmers präzise ermittelt und zu Marketingzwecken genutzt werden. Ohne Anonymität stünde grundsätzlich ein wirkungsvolles Instrument zur Verfügung, in geschützte Bereiche der Privatsphäre einzudringen.

2.2 Anforderungen an Zahlungsmethoden im Internet

Unabhängig von den Realisierungsmöglichkeiten eines Internet-EPS (siehe Kapitel 3) sind im Vergleich zu realem Geld die folgenden spezifischen Anforderungen an die Zahlungsmethoden mit elektronischem Geld zu stellen:

Transaktionssicherheit

An sichere Transaktionen sind die Bedingungen Vertraulichkeit (die Transaktion ist nicht unbefugt abhörbar), Integrität (die Transaktion ist nicht unbefugt manipulierbar), Authentizität (die an der Transaktion Beteiligten sind eindeutig identifizierbar) und Verbindlichkeit (die Transaktion ist nachvollziehbar und nicht bestreitbar) zu stellen. Neben diesen Sicherheitsbedingungen sollte das zugrundeliegende Transaktionsverfahren auch Schutz vor Fehlfunktionen durch Überlastung oder technischen Ausfällen bieten (Verfügbarkeit).[9] (Aufgrund der fundamentalen Bedeutung der Transaktionssicherheit für ein Internet-EPS befaßt sich Kapitel 2.3 eigens und näher mit dieser Anforderung.)

Benutzerfreundlichkeit

Zur Tauglichkeit für den breiten Masseneinsatz ist die Benutzerfreundlichkeit des Zahlungsverfahrens eine wesentliche Anforderung. Die Bezahlung muß per „click and pay button“ geschehen. Hierfür sollte es möglich sein, das Internet-EPS in das bestehende aktuelle World Wide Web (WWW) mit allen gängigen Browsern unter HTML sowie in kommende WWW-Technologien (z. B. Java) einzubinden.[10]

Kostengünstigkeit

Die Kosten der für die Nutzung des Internet-EPS auf Anbieterseite notwendigen Soft- und Hardware dürfen keine Prohibitivwirkungen auf „kleine“ Anbieter (micromerchants) entfalten. Zudem sollten die Transaktionskosten so gering sein, daß auch Micropayments interessant bleiben.

---

8 Vgl. Peirce, Michael; O'Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, Online in Internet: URL: http://www.w3.org/pub/Conferences/WWW4/Papers/228/ [Stand 19.2.96].

9 Vgl. Janson, P.; Waidner, M., Electronic Payment over Open Networks, Online im Internet: URL: http://www.zurich.ibm.ch/Technology/Security/publications/1995/JaWa95.dir/JaWa95e.html [Stand 20.2.96].

10 Vgl. Peirce, Michael; O'Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

Skalierbarkeit

Das Internet-EPS muß in der Lage sein, den weltweiten Einsatz mit heute bereits bis zu 40 Mio. Benutzern unterstützen zu können und beliebig ausbaubar zu sein, ohne die Leistungsfähigkeit des Systems zu beeinträchtigen (scalability).[11] Neben dieser teilnehmerorientierten Sichtweise der Skalierbarkeit wird ein exponentielles Wachstum der elektronischen Geldmenge zu bewältigen sein.

Plattformunabhängigkeit

Unter technischen Aspekten ist das Internet-EPS als offenes System zu gestalten. Alle Applikationen, Netzwerkprotokolle und Sicherheitsmechanismen müssen unabhängig von der benutzten Hardware mit jeder Systemsoftware implementierbar sein.

2.3 Transaktionssicherheit durch kryptographische Systeme

2.3.1 Sicherheit im Internet

„True digital cash (...) depends upon the marriage of economics and cryptography".[12] Sinnvolle **kryptographische Systeme** ver- und entschlüsseln die zu übertragenden Daten und kontrollieren nach der Übertragung die Echtheit der Daten und Kommunikationspartner. Die Kapitel 2.3.2 und 2.3.3 charakterisieren einige kryptograhische Problembereiche. Rechtliche und wirtschaftliche Hürden für kryptographische Systeme zeigen sich in Exporthemmnissen und lokalen Kryptographie-Verboten. So ist in einigen Ländern, darunter auch Frankreich, der Einsatz von kryptographischen Systemen in öffentlichen Netzen generell unzulässig. Unter das Exportverbot der USA für Waffen und Munition fällt auch der Export von kryptographischen Verfahren mit Schlüssellängen von mehr als 40 Bit. Für eine ausreichende Sicherheit sind aktuell jedoch Schlüssellängen von mindestens 128 Bit erforderlich.[13] EPS-Anbieter sind daher gezwungen, auf „kleine", nicht ausreichend sichere Schlüssel zurückzugreifen, Exportverbote durch die teure Eigenentwicklung von Verschlüsselungsmechanismen zu umgehen oder proprietäre Verschlüsselungskonzepte zu verwenden.

Je mehr Transaktionssicherheit im Internet verlangt wird, desto mehr kryptographischer und organisatorischer Aufwand muß betrieben werden und desto komplizierter werden die Zahlungsvorgänge. Die Sicherheitsmechanismen sind jedoch so auszulegen, daß die Komplexität des EPS nicht seine Leitsungsfähigkeit und Benutzerfreundlichkeit beeinträchtigt. Zur Unterbindung unbefugter Eingriffe müssen gleichzeitig die Kosten für das Umgehen der Sicherheitsmechanismen den zu erwartenden Nutzen prohibitiv übersteigen.

11 Vgl. Peirce, Michael; O'Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

12 Matonis, Jon W.: Digital Cash & Monetary Freedom, Online im Internet: URL: http://www.isoc.org /in95prc/HMP/PAPER/136/html/paper.html [Stand 2.3.96].

13 Vgl. o.V.: From Cowrie Shells to Digital Cash, Online im Internet: URL: http://cyberia.ie/internet /MechanismsForPaymentAndSecurity.html#security [Stand: 2.3.96].

2.3.2 Sicherheit durch Datenverschlüsselung mit Single- und Public-Keys

Kryptographische Systeme bedienen sich mathematischer Verfahren, um originale Zeichenketten eines Absenders in Zeichenketten umzuwandeln, die ausschließlich vom Empfänger wieder in den lesbaren Originalzustand versetzt werden können und somit für Dritte unverständlich sind. Für ein Internet-EPS muß vom Empfänger zudem die Authentizität des Absenders und die Manipulationsfreiheit der Daten festgestellt werden können.

Bei **Single-Key-Verfahren (symmetrische Verfahren)** werden Informationen mit einem einzigen Schlüssel kryptographiert und dechiffriert.[14] Insbesondere Banken und Versicherungen verwenden symmetrische Verfahren wie z. B. DES (Data Encryption Standard) zur Verschlüsselung von persönlichen Identifikationsnummern (PINs). Voraussetzung für diese Verfahren ist, daß ein sicherer Weg zur Übertragung des Schlüssels zwischen Absender und Empfänger existiert. Symmetrische Verfahren eignen sich daher kaum für den Datenaustausch zwischen anonymen Handelspartnern im Internet.

Mit **asymmetrischen Public-Key-Verfahren** (RSA-Systeme; Rivest-Shamir-Adleman) wird vermieden, einen Schlüssel auf einem sicheren Kanal zwischen den Kommunikationspartern übermitteln zu müssen. Informationen werden mit einem öffentlich bekannten Schlüssel chiffriert und mit einem privat erzeugten und geheim zu haltenden Schlüssel dechiffriert. Public-Key-Verfahren beinhalten die Möglichkeit mit Hilfe sogenannter Digital Signatures dafür zu garantieren, daß ein Dokument seit der digitalen Unterschrift nicht verändert wurde (not altered/not tampered). Weiterhin kann mit dem Public Key überprüft werden, ob eine Nachricht wirklich von einem bestimmten Absender stammt (authentication). **PGP (Pretty Good Privacy)** z. B. stellt eine Public-Domain-Realisierung des Public-Key-Verfahrens dar, die sich zur Verschlüsselung vom eMails weitgehend durchgesetzt hat. Die Sicherheit von PGP hängt von der Länge des verwendeten Schlüssels ab. Die Kosten für die Entschlüsselung eines 512-Bit-Keys ohne Kenntnis des privaten Schlüssels über das Nachvollziehen der zugrundeliegenden mathematischen Chiffrier-Verfahren mit leistungsfähigen Computern werden aktuell (Anfang 1996) auf ca. 8,2 Mio. US$ geschätzt.[15] Diese Kosten fallen jedoch mit permanent steigenden Rechnerleistungsfähigkeiten. Die verwendeten Schlüssel müssen daher gleichlaufend verlängert werden, um eine konstant ausreichende Sicherheit zu gewährleisten.

2.3.3 Sicherheit durch Protokoll-Verschlüsselung

Ergänzend zur Verschickung verschlüsselter Daten mit allgemein bekannten Protokollen im World Wide Web bietet sich die Möglichkeit, die verwendeten Protokolle selbst mit Verschlüsselungsmechanismen zu versehen (siehe Abbildung 1).

HTTP, das aktuell verwendete Protokoll auf der Anwendungsebene des World Wide Web, erlaubt zwar die Abfrage von Usernamen und Passwort (basis authentication), die

14 Vgl. Fox, Dirk: Schlüsseldienst-Private Kommunikation mit PEM und PGP, in: c't, 9/1995, S. 184.

15 Vgl. Dahl, Andrew; Lenick, Leslie: Internet Commerce, Indianapolis USA 1996, S. 145f.

diesbezüglichen Daten werden jedoch von HTTP selbst nicht durch Verschlüsselung gesichert.[16] Alle Daten werden über abhörbare Netzkanäle mit einem nachvollziehbaren Anwendungsprotokoll (HTTP) übertragen. **S-HTTP (Secure HTTP)** von Terisa Systems nimmt eine Erweiterung des HTTP-Standards auf der Anwendungsebene des WWW-Browsers vor, bevor die HTTP-Daten an die Verbindungsebene zur Versendung weitergeben werden. Im Grunde werden weiterhin HTTP-Nachrichten erzeugt, die jedoch in **gesicherte Protokoll-Hüllen eingekapselt** sind. Vorangestellte Kapselinformationen geben Auskunft über die im Hülleninneren verwendeten kryptographischen Verfahren für digitale Unterschriften, Datenverschlüsselung und Authentifizierung. Die Verschlüsselungsverfahren selbst sind nicht in das Protokoll integriert, sondern werden bei den beteiligten Kommunikationspartnern lokal gehalten.

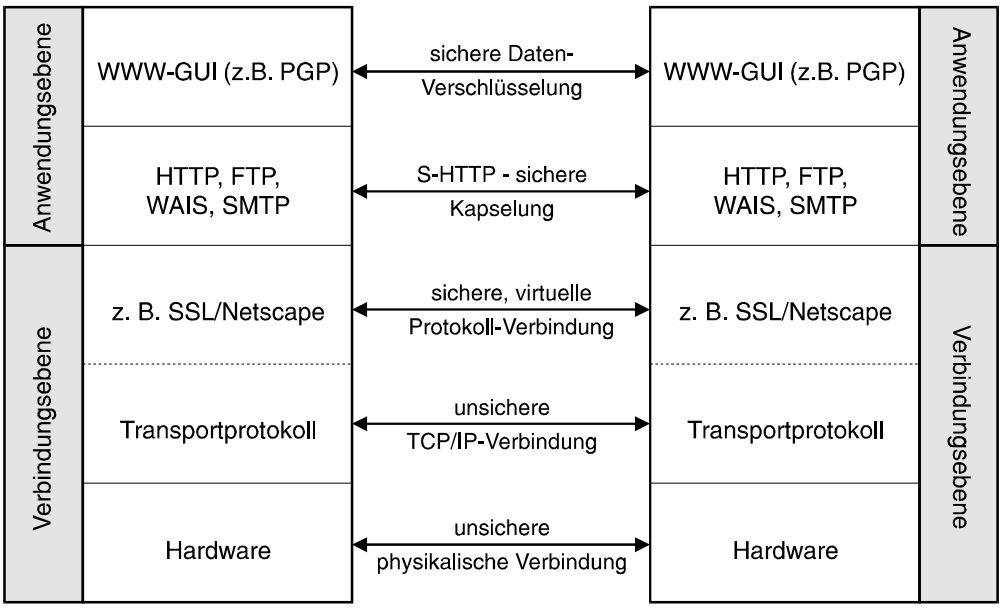

Abb. 1: Daten-Verschlüsselung und Protokoll-Verschlüsselung

Das **Secure Sockets Layer (SSL) Protocol von Netscape** setzt auf der Verbindungsebene (Sockets; Transportprotokoll) an, indem es das verwendete Transportprotokoll um einen gesicherten Kanal erweitert. SSL ist damit nicht nur für HTTP-Daten des World Wide Web nutzbar, sondern stellt seine Sicherheitsfunktion auch anderen Diensten der Anwendungsebene zur Verfügung. Ein gravierender Nachteil des SSL ist, daß es aufgrund des implementierten 128-Bit Keys der US-Exportrestriktion unterliegt. Die für den internationalen Markt bestimmte Variante besitzt lediglich einen 40-Bit Key, der für EPS-Transaktionen nicht ausreichend sicher ist.

Für eine Reihe weiterer Protokollsicherungsverfahren, die sich in Entwicklung befinden seien genannt: IPv6, die nächste Version des gültigen IP mit der Sicherheitsarchitektur IPSEC, Secure Electronic Transaction SET von Visa und MasterCard und das Private Communication Technology Protocol PCT von Microsoft.

16 Klute, Rainer: Verschlußsache - Sicherheit im World Wide Web, Online im Internet: URL: http://www.ix.de/ix/951232/default.html [Stand. 17.3.96].

3 Realisierungen von Electronic-Payment-Systemen

3.1 Modelle zur Realisierung von Electronic-Payment-Systemen

Sowohl Zahlungsmittel als auch Zahlungsmethoden eines Internet-EPS können auf dem herkömmlichen Zahlungssystem aufsetzen. Reales Geld wird dabei in elektronisches Geld umgetauscht, welches mit elektronischen Methoden übergeben und bei Bedarf wieder in reales Geld umgetauscht wird. Dazu kann auf vorhandene Infrastrukturen, z. B. die von Geschäftsbanken oder von Kreditkartengesellschaften, zurückgegriffen werden. Ein Internet-EPS kann daher allein aus einem Verfahren zum sicheren Übertragen von Kreditkarteninformationen bestehen **(Kreditkartensysteme mit secure credit card transactions)** oder mit sicheren Internet-Transaktionen des Bankensystem arbeiten **(debit/credit Systeme).**

Während die Kreditkarten- und debit/credit-Systeme auf den vorhandenen staatlichen Währungen (Notational Money) aufsetzen und ihre Leistung in der Übermittlung der Zahlungsinformation sowie den Verbindungen zu Banken besteht, werden bei **elektronischen Währungssystemen** eigenständige Zahlungsmittel (Electronic Currency) emittiert, die Internet-spezifische Übergabemethoden verwenden.[17] Diese „privaten“ Zahlungsmittel (Private Currency Units) können ggfs. in nationale Währungen oder andere „private“ Zahlungsmittel getauscht werden. Genausogut ist es aber auch vorstellbar, daß z. B. global aktive Unternehmen eigene elektronische Währungen ohne Konvertibilität in nationale Währungen schaffen.[18]

Die politischen, gesellschaftlichen und wirtschaftlichen Implikationen einer weltweit einheitlichen und eigenständigen Internet-Währung deuten auf die Notwendigkeit eines globalen Netzes multilateraler Abstimmungen zwischen den Emittenten nationaler Währungen hin. Vor dem Hintergrund der dafür erforderlichen immensen Anstrengungen erscheint es aktuell wenig sinnvoll, elektronische Währungen zu schaffen, die nicht auf den Konvertierungssystemen der existierenden staatlichen Währungen aufsetzen.

3.2 Kreditkarten-Systeme

Bei Kreditkarten-Systemen funktioniert das Bezahlen ähnlich wie beim Teleordering per Telefon. Durch Übergabe der Kreditkarten-Informationen (KK-Infos) an den Verkäufer kann dieser das Geld vom Kreditkarten-Emittent (KK-Emittent) einfordern, ohne daß hierfür eine Unterschrift des Käufers notwendig ist. Da die eigentliche Geldübertragung später über die vorhandene Infrastruktur des Kreditkarten-Emittenten geschieht, stehen Systeme zur Bezahlung mit Kreditkarte in der Hauptsache dem Problem der sicheren Übertragung der Kreditkarten-Informationen vom Käufer zum Verkäufer gegenüber.[19]

17 Vgl. Reif, Holger: Elektronischer Handel: Zahlungsmöglichkeiten im Internet, Online im Internet: URL: http://www.Praktinfo.fu.ilmenau.de/~reif/wsk195.ps [Stand: 10.4.96].

18 Vgl. Matonis, Jon W.: Digital Cash & Monetary Freedom, a. a. O.

19 Vgl. Reif, Holger: Elektronischer Handel: Zahlungsmöglichkeiten im Internet, a. a. O.

Dieses Problem kann entweder durch die Verwendung allgemein sicherer Transportdienste wie SSL, S-HTTP oder IPv6 für den gesamten Datenaustausch oder über die Verschlüsselung lediglich der sicherheitsrelevanten Daten vor dem Versenden, z. B. mit PGP, gelöst werden. Als weitere Möglichkeit bietet sich die Verwendung von speziellen Protokollen an, wie SET von Visa und MasterCard. Über dieses sich noch in der Entwicklungsphase befindlichen Protokoll sind zum aktuellen Zeitpunkt (April 1996) noch kaum Informationen verfügbar.[20] Bei anderen Kreditkarten-Systemen werden die Kreditkarten-Informationen nicht vom Käufer selbst, sondern vom EPS-Service-Anbieter an den Verkäufer gesendet. Bei diesen Systemen mit einer zentralen Verwaltung der Daten müssen Käufer und Verkäufer nur mit der zentralen Stelle ein kryptographisches Verfahren vereinbaren.

Abbildung 2 zeigt die Konzeption des EPS für Kreditkarten am Beispiel von **Cybercash** Der Cybercash Secure Internet Payment Service for credit cards enthält integrierte Kryptomechanismen mit Schlüssellängen von 768 Bit und kann sowohl SSL als auch S-HTTP Verbindungen nutzen. Diese Krypto-Mechanismen werden auch in den konkurrierenden Systemen von CheckFree und Compuserve (Compuserve wallet) angewendet.[21]

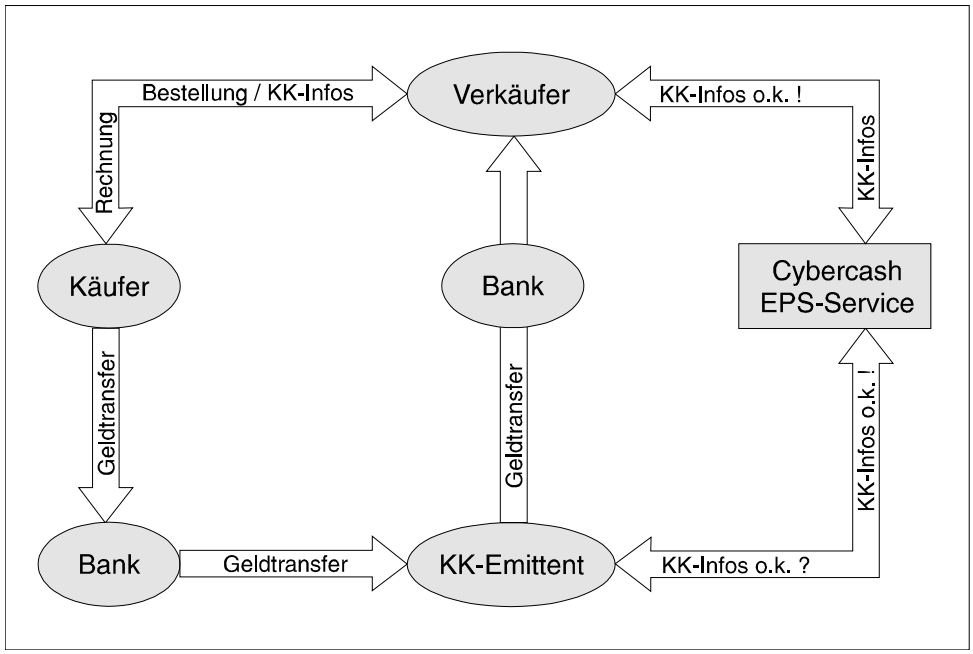

Abb. 2: Kreditkarten-System am Beispiel von Cybercash

Der Käufer wählt Artikel aus und startet seine **Cybercash-Wallet-Software.** Die Wallet-Software informiert den Verkäufer über den Verkaufsvorgang; der Verkäufer stellt daraufhin eine Rechnung. Der Käufer trägt seine Kreditkarten-Informationen in die Rechnung ein. Diese Informationen werden nun mit dem Cybercash-Public-Key-Verfahren verschlüsselt und an den Verkäufer zurückgeschickt; dieser ist dabei nicht in

20 Vgl. Reif, Holger: Elektronischer Handel: Zahlungsmöglichkeiten im Internet, a. a. O.

21 Vgl. o.V.: The Six Steps in a Secure Internet Credit Card Payment, Online im Internet: URL: http://www.cybercash.com/ho-we-are/sixsteps.html [Stand: 27.2.96].

der Lage, die privaten Informationen des Käufers einzusehen. Der Verkäufer fügt seine eigenen Identifikationsinformationen hinzu und sendet das Paket verschlüsselt an Cybercash, das eine Prüfung der Kreditkarte in Kooperation mit dem Kreditkarten-Emittenten vornimmt. Ist die Karte in Ordnung erhält der Verkäufer eine diesbezügliche Bestätigung. Da der Verkäufer auch hier keine weiteren Informationen über den Käufer erhält, bleibt dieser somit gegenüber dem Verkäufer anonym.[22] Der Geldtransfer geschieht nachfolgend über die Infrastruktur des Kreditkarten-Emittenten.

- Grundsätzlich läßt sich diese Zahlungsart mit der Benutzung von Kreditkarten im Offline-Geschehen außerhalb des Netzes vergleichen.
- Da für die Autorisierung verschiedener Kreditkarten(-Emittenten) meist Mindestgebühren (z. B. bei den Cybercash-Partnern) verlangt werden, eignen sich solche Systeme weniger für Micropayments.
- Die benötigte Wallet-Software wird an den Käufer meist kostenlos abgegeben.
- Ein großer Vorteil von Kreditkartensystemen ist zum einen die Unabhängigkeit von Währungen, da der Umtausch direkt vom Kreditkarten-Emittenten vorgenommen wird.
- Zum anderen wird der Kunde vor betrügerischen Händlern geschützt. Wenn der Verkäufer nach Übermittlung der Zahlungsinformationen die gewünschte Leistung nicht erbringt, kann der Käufer zumindest innerhalb einer bestimmten Frist versuchen, über sein Kreditkartenunternehmen die Durchführung der Zahlung zu unterbinden.
- Diesbezüglich hat das System auch Vorteile für Händler; ein Merkmal von Kreditkartensystemen ist, daß alle Transaktionen vom Kreditkarten-Emittenten versichert sind.
- Ein Nachteil der Kreditkarten-Systeme liegt in einer nur teilweisen Anonymität. Zwar bieten die Systeme eine Anonymisierung zwischen Käufer und Verkäufer; der Kreditkarten-Emittent bleibt allerdings immer über alle Transaktionen informiert.

3.3 Debit-/Credit-Systeme

Debit-Systeme funktionieren ähnlich wie ein Girokonto mit EC-Karte. Der Käufer muß bei seinem EPS-Service ein Konto eröffnen, über das die Verrechnung der Geldbeträge erfolgt. Hierauf muß zunächst reales Geld eingezahlt werden, bevor es im Internet ausgeben kann (prepaid); es muß stets ein ausreichender Geldbetrag auf dem Konto gehalten werden. Nach Vereinbarung kann der EPS-Service-Anbieter per Bankeinzug oder Kreditkarte den Kontostand ausgleichen, falls ein Limit unterschritten wird.

Bei **Credit-Systemen** erfolgt die Abrechnung nach dem Prinzip „kauf´ heute - zahl´ morgen“. Die für Käufe erforderlichen Beträge werden vom EPS-Service-Anbieter „vorgestreckt“ und zu einem vereinbarten Zeitpunkt von einem regulären Bankkonto abgebucht. Abbildung 3 zeigt die entsprechenden Vorgänge am Beispiel des **First Vir-**

22 Vgl. o.V.: From Cowrie Shells to Digital Cash, a. a. O.

tual Systems. Zunächst sendet der Käufer seine Bestellung und seine persönliche First-Virtual-Identification (FV-ID) unverschlüsselt an den Verkäufer, der letztere an First Virtual weiterleitet. First Virtual schickt nun dem Käufer ein eMail indem dieser aufgefordert wird, die Zahlung zu bestätigen. Bestätigt der Käufer, wird der Betrag dem First Virtual Konto des Händlers gutgeschrieben.[23]

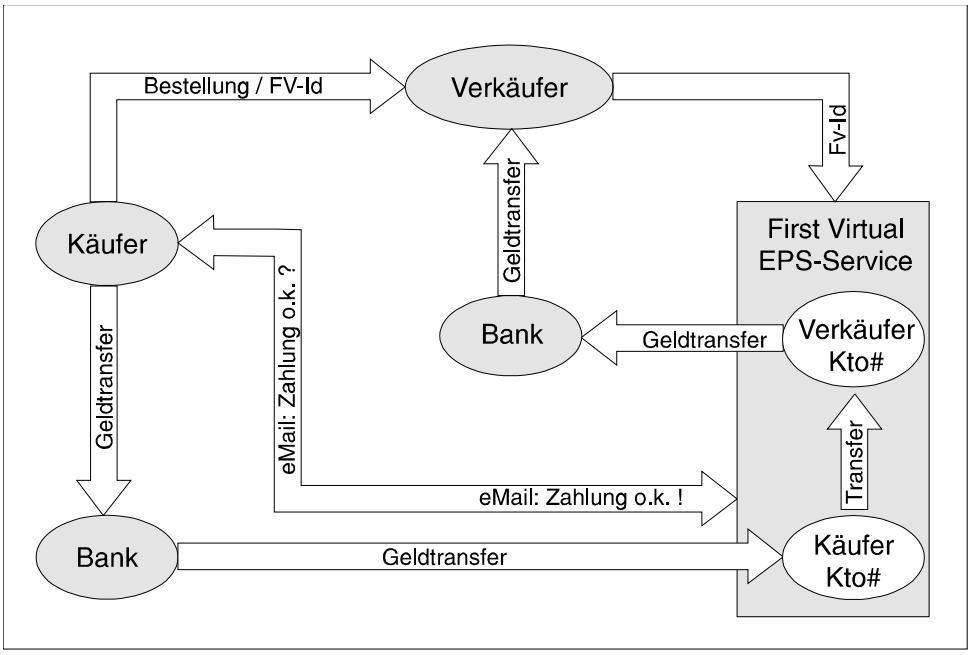

Abb. 3: Debit-Credit-System am Beispiel von First Virtual

Während der Zahlungsvorgang hier auf einem niedrigen Sicherheitsniveau lediglich durch eine eMail-Antwort autorisiert wird, benutzen andere Debit-/Credit-Systeme Online-Authorisierungsmechanismen. So beispielsweise das System von **Netbill,** bei dem nach der Bestellung einer Informationsleistung diese verschlüsselt auf den Rechner des Käufers gelegt werden. Erst nachdem der Netbill-EPS-Service den Zahlungsvorgang bestätigt hat, erhält der Kunde den Schlüssel für die Dechiffrierung.[24] Elektronische Einkaufszentren (full merchant solution) wie Open Market benutzen wiederum ein anderes System. Hier wird mit dem Einkaufszentrum im voraus eine Autorisierung für alle integrierten virtuellen Läden vorgenommen. Der Käufer zahlt nicht in jedem virtuellen Laden einzeln, sondern das Open-Market-System übernimmt die Abbuchung des Gesamt-Rechnungsbetrages von einem Bankkonto oder einer Kreditkarte des Kunden nachdem alle Einkäufe getätigt wurden und führt ggfs. die Überweisungen auf die Bankkonten der Verkäufer aus.[25] Beim **NetChex** System schreibt der Käufer elektroni-

23 Vgl. Stein, Lee H.; Stefferud, Einar A.; Borenstein, Nathaniel S.; Rose, Marshall T.: The Green Commerce Model, Online im Internet: URL: http://www.fv.com:80/pubdocs/green-model.txt [Stand 19.2.96].

24 Vgl. o.V.: The Netbill Overview, Online im Internet: URL: http://www.ini.cmu.edu/informations /CompCon_TOC.html [Stand: 20.2.96].

25 Vgl. o.V.: Conducting Secure, Effective Business on the World Wide Web, Online im Internet: URL: http://www.openmarket.com/products/merchsol/execwp.htm [Stand 19.3.96].

sche Schecks gegen sein NetChex-Konto aus, die der Händler dann als regulären Papierscheck per Post zugeschickt bekommt.[26]

- Debit-/Credit-Systeme eignen sich sowohl für kleinere, als auch für größere Beträge, da lediglich relativ geringe Kontoführungs- und EPS-Gebühren fällig werden.
- Die notwendige Front-End-Software für Käufer und Verkäufer wird meist kostenlos abgegeben.
- Ein Vorteil der Systeme mit rückfragender eMail-Autorisierung ist, daß diese nicht auf Probleme mit gesetzlichen Kryptographie-Verboten stoßen.
- Bisher setzen Debit-Credit-Systeme jedoch ein Bankkonto des Käufers bei einer US-Bank voraus und können daher nur bedingt außerhalb der USA angewandt werden.
- Anonymität ist nur zwischen Käufer und Verkäufer gegeben; die EPS-Service-Anbieter verfügen hingegen über detaillierte Kentnisse zu allen Zahlungsvorgänge.

3.4 Digital Cash - Elektronische Währungssysteme

Elektronische Währungssysteme funktionieren wie Papiergeld und Münzen, mit dem Unterschied, daß die Wertrepräsentanten sog. „Token“ in Form von Bitstrings sind.[27] Die Token enthalten eine Seriennummer, die Wertangabe und Hinweise zu der ausstellenden Institution. Ein Token stellt somit das elektronische Äquivalent zu „echtem“ Geld[28] dar. Elektronische Währungssysteme setzen den Trend der Geldentwicklung zu einer immer weitergehenden Entfernung von physisch existenten Werteinheiten zur Abstraktivität fort.[29] Token können zwischen beliebigen Rechnern übertragen werden, wodurch auch ein bilateraler Geldtransfer zwischen Privatpersonen möglich wird. **Anonymous Digital Cash** entspricht bezüglich der Anonymität dem konventionellen Papiergeld. Im Gegensatz dazu enthält **Identified Digital Cash**[30] Informationen über die Identität der Person, die ursprünglich das Geld von der ausgebenden Institution erhalten hat.

Ein Hauptproblem elektronischer Währungssysteme liegt im sogenannten Double Spending begründet. Verfügt der Käufer über Digital Cash auf seiner Festplatte, kann er versuchen, die Token zu kopieren und mehrfach auszugeben. Online-Systeme verhindern Double Spending durch eine Überprüfung der Token mittels direkter Interaktion mit dem Tokenaussteller. Dieser hält entweder die Seriennummern bereits benutzter Token, oder diejenigen noch gültiger Token in Datenbanken gespeichert, um sie mit der Seriennummer des zu prüfenden Token zu vergleichen.[31]

---

26 Vgl. Dahl, Andrew; Lenick, Leslie: Internet Commerce, a. a. O., S. 110.

27 Vgl. Reif, Holger: Elektronischer Handel: Zahlungsmöglichkeiten im Internet, a. a. O.

28 Vgl. Peirce, Michael; O’Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

29 Vgl. Sanders, Franklin: E-Money - Paradise or Prison?, Online im Internet: URL: http://com.primenet.com/callme/coins/emoney.html [Stand: 27.2.96].

30 Vgl. Miller, Jim: Digital Cash Mini-FAQ, Online im Internet: URL: http://ganges.cs.tcd.ie/mepeirce/Projekt/Mlists/minifaq.html [Stand 2.3.96].

31 Vgl. Miller, Jim: Digital Cash Mini-FAQ, a. a. O.

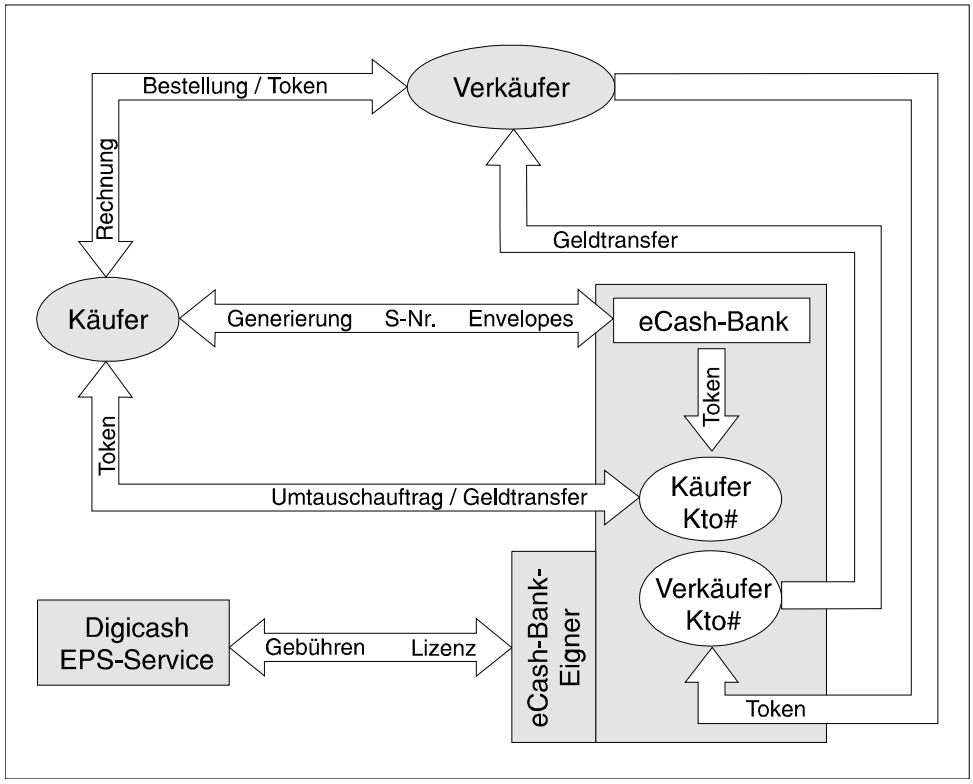

Abb. 4: Elektronisches Währungssystem am Beispiel von Digicash

Das holländische Unternehmen **Digicash** bietet mit eCash eine elektronische Währung an (siehe Abbildung 4). Digicash selbst will nicht als Aussteller von **eCash-Token** in Aktion treten, sondern dies anderen Institutionen überlassen, die dafür Lizenzgebühren zahlen sollen.[32] Als solche war die Mark Twain Bank die erste Bank, die eCash-Token auf Grundlage des US-Dollars ausstellte.[33] Käufer und Verkäufer benötigen die eCash-Software „Cyberwallet“, die kostenlos bereitgestellt wird, sowie jeweils ein Konto bei der eCash-Bank. Zu diesem Konto gehört eine digitale Unterschrift, die benutzt wird um die Seriennummern der Token zu erstellen. Der Umtausch des auf das eCash-Konto eingezahlten regulären Geldes geschieht wie folgt: Der Kontoinhaber unterschreibt den Umtauschauftrag mit seiner digitalen Unterschrift und übermittelt diesen über das Netz an die eCash-Bank. Diese prüft die Unterschrift und fordert den Rechner des Kontoinhabers auf, Seriennummern zu erstellen. Der Rechner des Kontoinhabers generiert die Seriennummern und schickt sie in sog. Envelopes an die Bank, die die Seriennummern nicht aus den Envelopes herauslesen kann (Anoymous Digital Cash). Mit einem Blind-Signature-Verfahren, das auf der Public-Key-Verschlüsselung aufbaut, unterschreibt die eCash-Bank die Seriennummern „durch die Envelopes hindurch" und bestätigt damit die

32 Vgl. Borchers, Detlef: Abrechnungs- und Zahlungsmodalitäten im Internet, a. a. O.

33 Vgl. o.V.: What is Ecash?, Online im Internet: URL: http://www.marktwain.com/whatis.html [Stand 20.2.96].

Gültigkeit der Token, die daraufhin an den Kunden geschickt werden.[34] Das elektronische Geld liegt nun auf der Festplatte des Kunden vor. Bei der Bezahlung mit eCash werden die Token durch die Cyberwallet-Software verschlüsselt und an den Verkäufer übermittelt.[35] Die Token-Gültigkeit prüft der Verkäufer, indem er sie an den eCash-Aussteller (the mint) sendet, der ihm ggfs. den betreffenden eCash-Betrag auf seinem Konto gutschreibt.

Ein alternatives elektronisches Währungssystem stellt **NetCash** vom Information Sciences Institute of the University of Southern California dar. Im Gegensatz zu Digicash handelt es sich hierbei um Identified Digital Cash, **„Coupons“** genannt. NetCash bietet keinen Schutz bei der Übertragung der Coupons, dieser muß durch PGP oder die Wahl eines sicheren Protokolls hergestellt werden.[36] Im Gegensatz zum Digicash-System, bei dem eCash wie Papiergeld über viele Besitzer hinweg im Umlauf bleiben kann, werden die NetCash-Coupons nach jedem Einsatz gegen neue eingetauscht.[37]

- Digital Cash eignet sich besonders für Micropayments, da keine Transaktionsgebühren anfallen.
- Im Gegensatz zu NetCash wahrt Digicash die Anonymität der an der Transaktion beteiligten Partner.
- Digicash und NetCash besitzen bisher kaum einen Schutz der Käufer vor Händlerbetrug, da die Token i. d. R. vor der Lieferung der Leistung übertragen werden.
- Der globale Einsatz wird im Falle von Digicash nicht durch US-Exportrestriktionen eingeengt, da der Firmensitz in den Niederlanden liegt.
- Zum einen verwendet Digicash jedoch Krypto-Verfahren, die in bestimmten Ländern nicht zulässig sind.
- Zum anderen wird sich eCash von Digicash (wie auch alle anderen Digital-Cash-Arten) als weltweites Internetzahlungsmittel nur durchsetzen können, wenn sich möglichst viele Banken einem bestimmten System anschließen und/oder die Systeme untereinander über konvertible elektronische Währungen verfügen.
- Im Vergleich zu den vorgenannten Kreditkarten- und Debit-/Credit-Systemen erfahren elektronische Währungssysteme einen immensen Attraktivitätszuwachs durch ihre Fähigkeit, Zahlungsmittel auch unter Privatpersonen austauschen zu können.
- Problematisch könnte sich das von Digicash benutzte Verfahren zur Sicherung vor Double Spending erweisen. Hierfür werden die Seriennummern aller bereits benutzter Token gespeichert, wodurch diese Datenbank permanent wachsen wird (Scalability Problem). Dieses Problem tritt durch eine andere Konzeption der Sicherung gegen Double Spending bei NetCash nicht auf.

---

34 Vgl. o.V.: DigiCash - Numbers That are Money, Online im Internet: URL: http://www.digicash.com /publish/digibro.html [Stand: 19.2.96]. Details zur Seriennummergenerierung und Verschlüsselung bei Bachem, A.; Heesen, R.; Pfenning, J.-T.: Digitales Geld für das Internet, in: ZfB, 6/1996, S. 707 f.

35 Vgl. Peirce, Michael; O’Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

36 Vgl. Peirce, Michael; O’Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

37 Vgl. Borchers, Detlef: Abrechnungs- und Zahlungsmodalitäten im Internet, a. a. O.

- Noch nicht ganz ausgereift sind die Mechanismen zum Schutz des Digital Cash auf den Festplatten der Nutzer.[38] Es darf nicht möglich sein, daß Dritte das dort vorgehaltene Digital Cash ausgeben oder entwenden können, auch wenn Zugriff auf den betreffenden Rechner besteht. Die Rekonstruktion von „verlorengegangenem" Digital Cash durch technische Defekte des lokalen Rechners stellt ein weiteres Problem dar.

Anstatt das elektronische Geld auf der Festplatte eines Rechners zu speichern, können **Smartcards** eingesetzt werden, die ähnlich wie Telefonkarten funktionieren. Die Smartcard besitzt einen Wächter (guardian), der eine Beeinflussung (tampering) des Geldstandes verhindern soll. Smartcards werden in Electronic-Wallet-Systemen eingesetzt; diese werden damit zum elektronischen Äquivalent der herkömmlichen Geldbörse. Die Verbindung eines Internet-EPS mit der „Brieftasche des normalen Lebens" bringt signifikante Mobilitätsvorteile mit sich, da der Nutzer nicht auf den Personal Computer angewiesen ist. Eine Smartcard kann jedoch mit Hilfe eines Readers über eine Schnittstelle an beliebige Rechner angeschlossen werden.

Ein Internet-taugliches Smartcard-System bietet **Mondex** an. Die Karte von Mondex kann bis zu 5 Währungen speichern und an einer Art Geldautomat aufgeladen werden. Eine direkte Übertragung des Geldes zwischen zwei Besitzern von Mondex-Karten ist über ein integriertes Lesegerät ohne weitere technische Übermittlungseinrichtungen möglich.[39] Ein konkurrierendes Smartcard-System mit dem Namen Cafe wird mit Förderung der EU von einem Firmenkonsortium um IBM und Cybercash entwickelt.[40]

4 Ausblick

Die potentiellen Gewinne für diejenigen EPS-Service-Anbieter, die die zukünftigen Standards setzen werden, sorgen dafür, daß der Innovationsprozeß weiter angetrieben wird. Der Markt für Internet-EPS wird sich dabei nicht auf ein System reduzieren lassen. Genau wie im konventionellen Geldverkehr wird sich im Internet ein Verbund aus Systemen für verschiedene Kundensegmente etablieren. Mittelfristig ist damit zu rechnen, daß EPS-Service-Anbieter kooperieren, um eine größere Segmentabdeckung zu erreichen. Die technische und funktionale Entwicklung einzelner Systeme ist dabei kaum zu prognostizieren. Die Entwicklungen der **nationalen Gesetzgebungen,** hier insbesondere die der US-amerikanischen, wird konstituierend für den Internet-Zahlungsverkehr sein. Die nationalen Regierungen sollten aus eigenem volkswirtschaftlichen Interesse schnellstmöglich die rechtlichen Grundlagen schaffen, damit angepaßte Verfahren und Techniken entwickelt und legal angewendet werden können. Vor diesem Hintergrund ist kaum damit zu rechnen, daß in Kürze ein allgemeiner und langlebiger Standard entstehen wird.

38 Vgl. Peirce, Michael; O'Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, a. a. O.

39 Vgl. o.V.: Mondex on the Internet, Online im Internet: URL: http://www.mondex.com/img/mondex /maps/pubbar.map?138,51 [Stand 27.2.96].

40 Vgl. o.V.: Digicash products - the CAFE project, Online im Internet: URL: http://www.digicash.com /products/projects/cafe.html [Stand 20.2.96].

Literaturverzeichnis

Bachem, A.; Heesen, R.; Pfenning, J.-T.: Digitales Geld für das Internet, in: ZfB, 6/1996, S. 697-712.

Borchers, Detlef: Abrechnungs- und Zahlungsmodalitäten im Internet - ein Überblick, Online im Internet: URL: http://www.ix.de/gw/gw9-95/internet/ecash.html [Stand 1.3.96].

Dahl, Andrew; Lenick, Leslie: Internet Commerce, Indianapolis USA 1996.

Fox, Dirk: Schlüsseldienst-Private Kommunikation mit PEM und PGP, in: c't, 9/1995, S. 184-187.

Fox, Dirk: Automatische Autogramme, Online im Internet: URL: http://www01.ix.de/artikel/ct9510/ Retorte.htm [Stand 9.2.96].

Janson, P.; Waidner, M.: Electronic Payment over Open Networks, Online im Internet: URL: http://www.zurich.ibm.ch/Technology/Security/publications/1995/JaWa95.dir/JaWa95e.html

Klute, Rainer: Verschlußsache - Sicherheit im World Wide Web, Online im Internet: URL: http://www.ix.de/ix/951232/default.html [Stand. 17.3.96].

Matonis, Jon W.: Digital Cash & Monetary Freedom, Online im Internet: URL: http://www.isoc.org/in95prc/HMP/PAPER/136/html/paper.html [Stand 2.3.96].

Miller, Jim: Digital Cash Mini-FAQ, Online im Internet: URL: http://ganges.cs.tcd.ie/mepeirce/Projekt/Mlists/minifaq.html [Stand 2.3.96].

o.V.: Conducting Secure, Effective Business on the World Wide Web, Online im Internet: URL: http://www.openmarket.com/products/merchsol/execwp.htm [Stand 19.3.96].

o.V.: DigiCash - Numbers That are Money, Online im Internet: URL: http://www.digicash.com/publish/digibro.html [Stand: 19.2.96].

o.V.: Digicash products - the CAFE project, Online im Internet: URL: http://www.digicash.com/products/projects/cafe.html [Stand 20.2.96].

o.V.: From Cowrie Shells to Digital Cash, Online im Internet: URL: http://cyberia.ie/internet/MechanismsForPaymentAndSecurity.html#security [Stand: 2.3.96].

o.V.: Mondex on the Internet, Online im Internet: URL: http://www.mondex.com/img/mondex/maps-/pubbar.map?138,51 [Stand 27.2.96].

o.V.: Survey on Internet Money, Online im Internet: URL: http://graph.ms.ic.ac.uk/analysis [Stand 2.3.96].

o.V.: The Six Steps in a Secure Internet Credit Card Payment, Online im Internet: URL: http://www.cybercash.com/ho-we-are/sixsteps.html [Stand: 27.2.96].

o.V.: The Netbill Overview, Online im Internet: URL: http://www.ini.cmu.edu/informations/CompCon_TOC.html [Stand: 20.2.96].

o.V.: What is Ecash?, Online im Internet: URL: http://www.marktwain.com/whatis.html [Stand 20.2.96].

Peirce, Michael; O'Mahony, Donald: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, Online in Internet: URL: http://www.w3.org/pub/Conferences/WWW4/Papers/228/ [Stand 19.2.96].

Reif, Holger: Netz ohne Angst, in: c't, 9/1995, S. 174-183.

Reif, Holger: Elektronischer Handel: Zahlungsmöglichkeiten im Internet, Online im Internet: URL: http://www.Praktinfo.fu.ilmenau.de/~reif/wsk195.ps [Stand: 10.4.96].

Rensmann, Jörg: Strukturchaos Internet, in: N&C, 12/1995, S. 56-63.

Sanders, Franklin: E-Money - Paradise or Prison?, Online im Internet: URL: http://com.primenet.com-/callme/coins/emoney.html [Stand: 27.2.96].

Schneider, Gerhard: Eine Einführung in das Internet, in: Informatik Spektrum, 18/1995, S. 263-271.

Stein, Lee H.; Stefferud, Einar A.; Borenstein, Nathaniel S.; Rose, Marshall T.: The Green Commerce Model, Online im Internet: URL: http://www.fv.com:80/pubdocs/green-model.txt [Stand 19.2.96].

Bisher erschienen

Stand: Dezember 2000 – Den aktuellen Stand der Reihe erfahren Sie über unsere Web Site unter http//wi.uni-giessen.de

Nr. 1/1996	Grundlagen des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 2/1996	Wettbewerbs- und Organisationsrelevanz des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 3/1996	Realisierungsaspekte des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 4/1996	Der Geschäftsprozeß als formaler Prozeß - Definition, Eigenschaften, Arten	Schwickert/Fischer
Nr. 5/1996	Manuelle und elektronische Vorgangssteuerung	Schwickert/Rey
Nr. 6/1996	Das Internet im Unternehmen - Neue Chancen und Risiken	Schwickert/Ramp
Nr. 7/1996	HTML und Java im World Wide Web	Gröning/Schwickert
Nr. 8/1996	Electronic-Payment-Systeme im Internet	Schwickert/Franke
Nr. 9/1996	Von der Prozeßorientierung zum Workflow-Management - Teil 1: Grundgedanken, Kernelemente, Kritik	Maurer
Nr. 10/1996	Von der Prozeßorientierung zum Workflow- Management - Teil 2: Prozeßmanagement und Workfflow	Maurer
Nr. 11/1996	Informationelle Unhygiene im Internet	Schwickert/Dietrich/Klein
Nr. 12/1996	Towards the theory of Virtual Organisations: A description of their formation and figure	Appel/Behr
Nr. 1/1997	Der Wandel von der DV-Abteilung zum IT-Profitcenter: Mehr als eine Umorganisation	Kargl
Nr. 2/1997	Der Online-Markt - Abgrenzung, Bestandteile, Kenngrößen	Schwickert/Pörtner
Nr. 3/1997	Netzwerkmanagement, OSI Framework und Internet SNMP	Klein/Schwickert
Nr. 4/1997	Künstliche Neuronale Netze - Einordnung, Klassifikation und Abgrenzung aus betriebswirtschaftlicher Sicht	Strecker/Schwickert
Nr. 5/1997	Sachzielintegration bei Prozeßgestaltungsmaßnahmen	Delnef
Nr. 6/1997	HTML, Java, ActiveX - Strukturen und Zusammenhänge	Schwickert/Dandl
Nr. 7/1997	Lotus Notes als Plattform für die Informationsversorgung von Beratungsunternehmen	Appel/Schwaab
Nr. 8/1997	Web Site Engineering - Modelltheoretische und methodische Erfahrungen aus der Praxis	Schwickert
Nr. 9/1997	Kritische Anmerkungen zur Prozeßorientierung	Maurer/Schwickert
Nr. 10/1997	Künstliche Neuronale Netze - Aufbau und Funktionsweise	Strecker
Nr. 11/1997	Workflow-Management-Systeme in virtuellen Unternehmen	Maurer/Schramke
Nr. 12/1997	CORBA-basierte Workflow-Architekturen - Die objektorientierte Kernanwendung der Bausparkasse Mainz AG	Maurer
Nr. 1/1998	Ökonomische Analyse Elektronischer Märkte	Steyer
Nr. 2/1998	Demokratiepolitische Potentiale des Internet in Deutschland	Muzic/Schwickert
Nr. 3/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 1)	Delnef
Nr. 4/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 2)	Delnef
Nr. 5/1998	Betriebswirtschaftlich-organisatorische Aspekte der Telearbeit	Polak
Nr. 6/1998	Das Controlling des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 7/1998	Eine kritische Beurteilung des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 8/1998	Online-Monitoring - Gewinnung und Verwertung von Online-Daten	Guba/Gebert
Nr. 9/1998	GUI - Graphical User Interface	Maul
Nr. 10/1998	Institutionenökonomische Grundlagen und Implikationen für Electronic Business	Schwickert
Nr. 11/1998	Zur Charakterisierung des Konstrukts “Web Site”	Schwickert
Nr. 12/1998	Web Site Engineering - Ein Komponentenmodell	Schwickert
Nr. 1/1999	Requirements Engineering im Web Site Engineering – Einordnung und Grundlagen	Schwickert/Wild
Nr. 2/1999	Electronic Commerce auf lokalen Märkten	Schwickert/Lüders
Nr. 3/1999	Intranet-basiertes Workgroup Computing	Kunow/Schwickert
Nr. 4/1999	Web-Portale: Stand und Entwicklungstendenzen	Schumacher/Schwickert
Nr. 5/1999	Web Site Security	Schwickert/Häusler
Nr. 6/1999	Wissensmanagement - Grundlagen und IT-Instrumentarium	Gaßen
Nr. 7/1999	Web Site Controlling	Schwickert/Beiser
Nr. 8/1999	Web Site Promotion	Schwickert/Arnold
Nr. 9/1999	Dokumenten-Management-Systeme – Eine Einführung	Dandl
Nr. 10/1999	Sicherheit von eBusiness-Anwendungen – Eine Fallstudie	Harper/Schwickert
Nr. 11/1999	Innovative Führungsinstrumente für die Informationsverarbeitung	Jäger-Goy
Nr. 12/1999	Objektorientierte Prozeßmodellierung mit der UML und EPK	Dandl
Nr. 1/2000	Total Cost of Ownership (TCO) – Ein Überblick	Wild/Herges
Nr. 2/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 1: XML-Grundlagen	Franke/Sulzbach
Nr. 3/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 2: Der Einsatz im Unternehmen	Franke/Sulzbach
Nr. 4/2000	Web-Site-spezifisches Requirements Engineering – Ein Formalisierungsansatz	Wild/Schwickert
Nr. 5/2000	Elektronische Marktplätze – Formen, Beteiligte, Zutrittsbarrieren	Schwickert/Pfeiffer
Nr. 6/2000	Web Site Monitoring – Teil 1: Einordnung, Handlungsebenen, Adressaten	Schwickert/Wendt
Nr. 7/2000	Web Site Monitoring – Teil 2: Datenquellen, Web-Logfile-Analyse, Logfile-Analyzer	Schwickert/Wendt
Nr. 8/2000	Controlling-Kennzahlen für Web Sites	Schwickert/Wendt
Nr. 9/2000	eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen	Schwickert/Ostheimer/Franke

Bestellung (bitte kopieren, ausfüllen, zusenden/zufaxen)

Adressat:

Professur für BWL und Wirtschaftsinformatik
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefax: (0 641) 99-22619

Hiermit bestelle ich gegen Rechnung die angegebenen Arbeitspapiere zu einem Kostenbeitrag von DM 10,- pro Exemplar (MwSt. entfällt) zzgl. DM 5,- Versandkosten pro Sendung.

Nr.	An
1/1996	
2/1996	
3/1996	
4/1996	
5/1996	
6/1996	
7/1996	
8/1996	
9/1996	
10/1996	
11/1996	
12/1996	

Nr.	An
1/1997	
2/1997	
3/1997	
4/1997	
5/1997	
6/1997	
7/1997	
8/1997	
9/1997	
10/1997	
11/1997	
12/1997	

Nr.	Anz
1/1998	
2/1998	
3/1998	
4/1998	
5/1998	
6/1998	
7/1998	
8/1998	
9/1998	
10/1998	
11/1998	
12/1998	

Nr.	Anz
1/1999	
2/1999	
3/1999	
4/1999	
5/1999	
6/1999	
7/1999	
8/1999	
9/1999	
10/1999	
11/1999	
12/1999	

Nr.	Anz
1/2000	
2/2000	
3/2000	
4/2000	
5/2000	
6/2000	
7/2000	
8/2000	
9/2000	

Absender:

_____
Organisation

_____
Abteilung

_____
Nachname, Vorname

_____
Straße

_____
Plz/Ort

_____
Telefon Telefax eMail

_____
Ort, Datum Unterschrift