Universität Konstanz
Informationswissenschaft
Postfach 5560
78457 Konstanz

Electronic Commerce: Konzepte, Standards und Entwicklung von interaktiven Transaktionsformen im Internet

Klaus Görke / Wolfgang Semar

Bericht 82-97

April 1997

ISSN 0942-2625

Universität Konstanz, Informationswissenschaft

Klaus Görke und Wolfgang Semar

Themengebiet: **Electronic Commerce: Konzepte, Standards und Entwicklung von interaktiven Transaktionsformen im Internet**

Abstract: Im Mittelpunkt der vorliegenden Projektarbeit steht die Beobachtung der Entwicklung interaktiver Transaktionsformen (Buchungen, Bestellungen, Zahlungsverkehr) in Online- bzw. Mehrwertdiensten. Nach einem Überblick auf die Sicherheitsproblematik im Internet werden die verschiedenen Verfahren und Standards des elektronischen Zahlungsverkehrs sowie des Electronic Internet Banking dargestellt und erörtert. Die sich abzeichnenden Entwicklungstendenzen werden dabei aufgezeigt und Möglichkeiten der Implementierung in elektronischen Märkten dargestellt.

0 INHALTSVERZEICHNIS

Abbildungsverzeichnis:

1. Einleitung

Der Trend zur kommerziellen Nutzung des Internets für kommerzielle Zwecke wird zunehmend stärker. Immer mehr Unternehmen drängen sich mit eigenständigen Applikationen in das Internet, um dessen Möglichkeiten für sich zu nutzen. Dies geschieht in vielen Fällen aus folgenden Gründen:

1. Aufbau einer Verbindung zum Internet mit dem Zweck der Informationsgewinnung;
2. Aufbau einer eigenen Präsenz aus Marketing-, Public-Relation- und Imagegesichtspunkten;
3. Integration der Internetverbindungen in die Geschäftsprozesse (z. B. externe Briefkommunikation über Email, Online-Bestellung, -Buchungen und -Verkauf).

Den letzten Schritt (3) wollen wir als interaktive Transaktionsformen (Bestellungen, Buchungen, Zahlungsverkehr) bezeichnen und näher betrachten. Sie stellt die weitgehendste Möglichkeit der Nutzung des Internets da. Für die Gesamtheit der Transaktionen, die über dieses Medium abgewickelt werden, wird weltweit ein 10faches Wachstum der Online-Umsätze für den Zeitraum von 1994 bis 2005 vorhergesagt[1], obwohl die Schwächen des Internets bezüglich Sicherung und Abwicklung von Zahlungen bekannt sind und allgemein interaktive Transaktionsformen, wie z. B. Bestellungen, Buchungen oder der elektronische Zahlungsverkehr, sich derzeit noch im Anfangsstadium der Entwicklung befinden. Elektronische Märkte und einzelne Anbieter präsentieren zwar ihre Produkte und Dienstleistungen aller Art in Form von virtuellen Schaufenstern, der eigentliche Prozeß des Kaufens und Bezahlens wird aber meist noch konventionell in Form von Überweisungsaufträgen per Nachnahme oder mittels Kreditkarte abgewickelt.

Die Nutzung des Internets für kommerzielle Zwecke ist immer noch Neuland, weshalb Anbieter im allgemeinen einen schrittweisen Ansatz zur Anbindung verfolgen. Dabei sind Sicherheitsbedenken zur Zeit immer noch die wesentliche Hemmnisse für den kommerziellen Einsatz. Durch die Entwicklung der Firewall-Technologie und der Erweiterung des Sockets und HTTP-Protokolls um Authentifizierung, Datenintegrität und -vertraulichkeit ist jedoch heute schon eine sichere Nutzung des Internets für den Informationsaustausch möglich. Neue

---

[1] Die Zahlen basieren auf Rechercheergebnisse und Veröffentlichungen des „Spiegels“ [Spi96].

Entwicklungen betreffen nun die Sicherung der Zahlungen auf dem Netz. Inzwischen gibt es eine Reihe verschiedener Systeme für elektronische Zahlungen, die zum Teil im Internet optional betrieben werden.

Nach einem Exkurs in Fragen der Sicherheit des Internets soll der Schwerpunkt auf die Sicherheitskonzepte der Anwendungen gelegt werden, die im Rahmen von interaktiven Transaktionsformen z. B. beim elektronischen Bestellen und Bezahlen benötigt werden. Der Hauptteil des theoretischen Teils der Arbeit besteht darin, die verschiedenen Standards und Konzepte für die Realisierung sicherer finanzieller Transaktionsformen in elektronischen Märkte zu kategorisieren, Kriterien der Akzeptanz bzw. Nutzung an bestehende Konzepte aufzuzeigen und zu erwartende Entwicklungstendenzen abzuleiten.

2. Sicherheitsaspekte im Internet

War die Technologie des Internets ursprünglich ausschließlich zum Zweck einer möglichst einfachen und offenen Verbindung von Rechnern gedacht, um einen möglichst freien Austausch von Informationen zwischen Wissenschaftlern und Forschungseinrichtungen zu erlauben - die unbehinderte Kommunikation wichtiger war, als die Belange der Sicherheit - so hat sich dies durch die zunehmende Forderung nach kommerzieller Nutzung stark verändert.

Die Sicherheitsrisiken des Internets liegen begründet:

1. im Mechanismus der Datenübertragung;
2. in den Diensten des Internets (Email, WWW, Telnet, FTP, Archie, Gopher, Whois, WAIS, Newsgroups).

Der Verbindungsaufbau über TCP/IP erfolgt, indem der Anrufer (Client) eine Anforderung (Request) an einen Teilnehmer (Server) sendet. Nach der Bestätigung des Servers können die Daten ausgetauscht werden. Hierbei werden die Daten in Pakete bestimmter Größe (max. 1500 Zeichen) unterteilt, vom Sender zum Empfänger weitergeleitet und am Zielort wieder zusammengesetzt. Dabei übernimmt das Internet Protocol (IP) die Funktion der Adressierung und stellt sicher, daß die Vermittlungsstellen (Router und Gateway) wissen, wohin die Datenpakete verschickt werden sollen. Die Datenpakete suchen sich dann eigenständig den Weg durch den funktionierenden Teil des Netzwerks und umgehen Teilbereiche, die außer Funktion sind. Der Weg der Pakete, die Route, ist demzufolge vorher nicht bekannt. Es läßt sich also nicht vorhersagen, bei welchen Internet-Hosts die Daten unterwegs vorbeikommen[2]. Somit kann der Sender nur hoffen, daß an den bei der Übertragung beteiligten Rechnern nur "vertrauenswürdige" Personen sitzen, welche die Daten nicht öffentlich bekannt machen (Geheimhaltung), den Inhalt der Pakete unverändert lassen (Unversehrtheit/Integrität) und keine fingierten Pakete hinzufügen (Echtheit) [Reif 95].

Eine sichere Lösung für die Sicherheitsproblematik im Internet wird erst dann gesehen, wenn die Internet Engineering Task Force (IETF) die Entwicklung von IPnG "Internet Protocol

---

[2] Das Quellrouting ermöglicht zwar eine explizite Angabe des Weges, ist aber weniger flexibel und läßt sich nicht immer anwenden.

Next Generation" abgeschlossen hat. Die Einführung des neuen IP[3] bedeutet einen gravierenden Einschnitt in die Technik des Internets und kann daher nur allmählich erfolgen. Motiviert ist sie vor allem durch das rasche Anwachsen des Netzes, das früher oder später einen größeren Adressierbereich benötigt[4]. Zu den zahlreichen Neuerungen von IPv6 werden auch zwei unabhängige Sicherheitsoptionen gehören. Eine soll Informationen zur Überprüfung von Authentizität und Integrität bereitstellen, die andere als Träger von Informationen zur Implementierung von Verschlüsselungsverfahren dienen [Smo95].

Bis heute wurden eine Reihe von Konzepten und Lösungswegen zur Erhöhung der Sicherheit und zur Ermöglichung interaktiver Transaktionen unter dem Stichwort „Electronic Commerce" entwickelt, die von verschiedenen Anbietern mit entsprechenden Produkten angeboten werden. Ein wichtiges kurzfristiges Ziel sind aber internationale Standardisierungen im Rahmen von Spezifikationen, Design- und Referenzimplementationen, die dem Nutzer sowohl auf der Anbieter-, als auch auf der Nachfragerseite, Sicherheit, Vertraulichkeit und Zuverlässigkeit bei interaktiven Transaktionen versprechen. Die verschiedenen Sicherheitskonzepte lassen sich dabei auf der Ebene der Sicherung des Netzes (Firewalls) und der Anwendungen und Applikationen im Internet differenzieren, wobei wir im Rahmen dieser Arbeit die Ebene der Anwendungen und Applikationen betrachten.

- Bei der einfachen Netzverbindung mit dem Internet öffnet man sein eigenes internes Netz dem Zugang von außen, so das sich die Frage der Kontrollierbarkeit des Zuganges stellt, zumal es im Bereich des Internets, seiner TCP/IP-Protokolle und den daran angeschlossenen Computern vielfältige Möglichkeiten des Einbruchs in vernetzte Systeme gibt. Die Sicherheit dieser Verbindung stellt erhöhte Anforderungen an die Kontrollierbarkeit der Kommunikationsdienste, die dem externen Nutzer angeboten werden und der Kontrolle des Datenverkehrs über diese Dienste.

- Werden Informationen im Netz zur Verfügung gestellt, erhöhen sich die Anforderungen je nach Art der Informationen um die Forderung nach Authentifizierung der Nutzer und / oder nach Integrität der übermittelten Daten, z. B. im Rahmen einer Online-Bestellung.

---

[3] Offiziell Version 6, derzeit ist IPv4 im Einsatz.

[4] IPnG wird einen Adressierbereich von 128 Bit, d. h. 2 Exp. 128 Adressiermöglichkeiten.

- Wird ein Netzzugang betrieben, der die eigenen Geschäftsprozesse integriert, um z. B. Online-Handel zu betreiben, kommen Forderungen nach gegenseitiger Authentifizierung der Kommunikationspartner, rechtsstabilen Unterschriften der Geschäftstransaktionen und adäquaten elektronischen Online-Zahlungsmöglichkeiten hinzu [Jan95].

2.1 Firewall-Technologie

Neben dem Einsatz von "File Integrity Checker", deren Aufgabe es ist, den Eigenbestand an Files gegenüber Viren zu schützen, gilt ein weiterer Ansatz dem Schutz des eigenen Netzes vor unbefugter Nutzung. Das Ziel, die Anzahl der Zugänge möglichst klein zu halten und gleichzeitig diese Zugänge entsprechend zu kontrollieren, führte zur Entwicklung sogenannter Firewalls, die folgende Funktionen anbieten:

- Trennung des Netzes in ein internes, sicheres und ein externes, unsicheres Netz;
- Kontrolle des Datenverkehrs zwischen externem und internem Netz, gegebenenfalls mit zugeschalteter Protokollierung;
- Geheimhaltung der Information über die interne Netzstruktur (z. B. Routing) an das externe Netz, um mögliche Ansatzpunkte zu verschleiern.

Im allgemeinen wird eine recht einfache Sicherheitspolitik beim Betrieb von Firewalls bevorzugt, die dem internen Anwender den Zugriff auf bestimmte externe Anwendungen erlaubt, dem externen Anwendern aber entweder keine oder nur den Email Zugang zum internen Netz gewährt. Die heute zur Verfügung stehenden Firewalls kommen häufig in der Kombination dreier Techniken zur Anwendung. Die Stichworte in diesem Bereich heißen: Paketfilter / Screening Router-Konfiguration, Application-Level Gateways (Proxy-Server) und Circuit-Level-Gateways[5]. Die Netzebene mit der Thematik des Netzschutzes und der angeschlossenen Systeme gegen Angriffe von außen soll im weiteren nicht vertieft werden. Die Sicherheitsfragen, mit denen wir uns beschäftigen, berühren die Ebene von Objekten, Benutzern, Servern und Clients. Fragestellungen wie z. B. "Wie können verbindliche Transaktionen über das Netz abgewickelt werden?", "Wie kann gewährleistet werden, daß

[5] Eine detaillierte Darstellung der Techniken von Firewalls und ihrer Architektur (Dual Home Bastion/Screening Subnet) wird an dieser Stelle nicht verfolgt [Kno96].

eine Information wirklich von der Person stammt, die vorgibt, der Urheber zu sein?", „Wie kann sichergestellt werden, daß eine Information nicht auf dem Weg zum Empfänger verändert wurde?", „Wie kann gewährleistet werden, daß nur der vorgesehene Adressat die Information liest?", „Wie kann gewährleistet werden, daß die Datenspuren, die die Benutzer in vielen zwischengeschalteten Systemen hinterlassen, nicht auf unerwünschte Weise verknüpft und ausgewertet werden?". Diese und andere Fragestellungen zeigen die Problematik bei der Einführung von interaktiven Transaktionsformen (elektronischer Zahlungsverkehr, Bestellungen und Buchungen) im Internet.

2.2 Kryptographie und Protokollspezifikationen

Werden über offene Netze elektronische Angebote und Bestellverfahren realisiert, so daß geldwerte Transaktionen durchgeführt oder Verträge abgeschlossen werden können, so sind Hilfsmittel notwendig, mit denen elektronische Handlungen auch gegenüber Dritten (z. B. vor Gericht) beweisbar gemacht werden können. Die Verantwortlichkeit im elektronischen Handel muß nachvollziehbar sein. Dabei sind die grundlegenden Sicherheitsanforderungen, abgeleitet aus den engl. Begriffen privacy, authentication, integrity of messages and non-repudiation (PAIN):

- Mechanismen, die die *Vertraulichkeit* von ausgetauschten Informationen sicherstellen (privacy);
- Mechanismen, die die *Authentizität* der Kommunikationspartner beweisen, auch gegenüber Dritten (authentication);
- Mechanismen, die die *Integrität* der ausgetauschten Information beweisen (Integrity of messages);
- Mechanismen, die die *Nicht-Rückweisbarkeit* und die *Verbindlichkeit* von ausgetauschten Informationen sicherstellen (non-repudiation).

2.2.1 Vertraulichkeit

Die Kommunikation zwischen zwei Parteien ist nur auf diese beschränkt, d.h. kein unbefugter Dritter darf Zugriff auf die ausgetauschten Informationen haben. Vertraulichkeit wird in offenen Netzwerken durch verschiedene kryptographische Verfahren unterstützt. Der Sender

verschlüsselt den Klartext und schickt das entstandene chiffrierte Datenpaket über das Netz zum Empfänger, der wiederum entschlüsselt es und erhält so den Klartext. Verschlüsselungsmechanismen werden grundsätzlich in symmetrische (Sender und Empfänger verwenden denselben Schlüssel) und asymmetrische (Sender und Empfänger besitzen unterschiedliche Schlüssel) Verfahren unterteilt.

2.2.2 Symmetrische Kryptographie

In der IETF, der Internet Engineering Task Force, in der alle technischen Verfahren und Standards des Internets entwickelt werden, wird gegenwärtig in der Arbeitsgruppe "IP Security" ein neuer Standard vorbereitet, der es erlaubt, das IP-Protokoll kryptographisch abzusichern. Will man die Vertraulichkeit einer Information bewahren, muß man sie verschlüsseln. Wenn der Empfänger denselben Schlüssel und dasselbe Verschlüsselungsverfahren anwendet wie der Sender, kann er die Information wieder entschlüsseln. Auf diese Weise funktionieren konventionelle oder *symmetrische* (auch *Private-Key-Verfahren*) kryptographische Systeme wie beispielsweise der ***Data Encryption Standard Algorithmus (DES)*** oder der ***International Data Encryption Algorithm (IDEA)***. Allerdings muß zwischen Sender und Empfänger ein gemeinsamer Schlüssel etabliert werden. Symmetrische Verschlüsselungen wie das DES-Verfahren haben aber das Problem des "shared secret". Um nachzuprüfen, ob der Sender im Besitz eines bestimmten Schlüssels ist, muß der Verifizierende genau diesen Schlüssel anwenden. Mindestens zwei Kommunikationspartner benutzen also denselben Schlüssel. Aus diesem Grund kann man den Ursprung einer Information nicht ausschließlich auf eine Person zurückführen.

2.2.3 Asymmetrische Kryptographie

Da symmetrische Algorithmen bereits häufiger „geknackt“ wurden, gelten die asymmetrischen Verfahren als sicherer. Diese erfordern aber eine komplexe Schlüsselverwaltung (Schlüsselgenerierung und -distribution), und zudem arbeiten die Algorithmen langsamer als die der symmetrischen Verschlüsselung. Der Vorteil bei asymmetrischen Verfahren ist aber die digitale Signatur. Für das Internet werden deshalb in mehreren Programmen diese Vorteile kombiniert.

Whitfield Diffie und Martin Hellmann haben in einem 1976 publizierten Artikel die Frage untersucht, ob man nicht mit einem 2-Schlüssel-System oder *asymmetrischem Kryptosystem*

arbeiten kann, bei dem man mit dem einen Schlüssel nachweisen kann, daß man den anderen Schlüssel besitzt, ohne diesen preisgeben zu müssen. Rivest, Shamir und Adleman haben dann 1978 einen Algorithmus publiziert, der genau diese Eigenschaft besitzt und als ***RSA-Algorithmus*** bekannt geworden ist [Sch96].

Bei asymmetrischen Kryptosystemen hat jeder Teilnehmer zwei komplementäre Schlüssel, einen öffentlichen (public-key) und einen geheimen Schlüssel (private-key). Jeder Schlüssel entschlüsselt das Chiffrat, das mit dem anderen hergestellt worden ist. Der private Schlüssel kann nicht aus dem öffentlichen Schlüssel abgeleitet werden. Der öffentliche Schlüssel kann daher über offene Netze verteilt und publiziert werden. Jeder kann eine Nachricht mit dem öffentlichen Schlüssel eines Empfängers verschlüsseln, und nur dieser kann sie mit seinem geheimen Schlüssel wieder lesen. Die Sicherheit asymmetrischer Verschlüsselungsalgorithmen beruht i.d.R. auf algebraischen Berechnungen, die schwierig umkehrbar sind (z. B. ist das Produkt zweier großer Primzahlen als Umkehrfunktion mit der Zerlegung dieser Zahl in ihre Primfaktoren aufwendiger). Auf der Primzahlzerlegung basiert der RSA-Algorithmus [Sch96 S.19]. Asymmetrische Algorithmen sind sehr rechenintensiv, deshalb werden nur kleinere Datenmengen mit RSA verschlüsselt, z. B. ein Hash-Wert zur Bildung einer digitalen Signatur, oder ein symmetrischer Verschlüsselungsschlüssel. Bei größeren Datenmengen werden symmetrische und asymmetrische Kryptographie in einem Hybridverfahren angewandt: man generiert einen symmetrischen Schlüssel, verschlüsselt damit die Daten und verschlüsselt anschließend den symmetrischen Schlüssel mit dem öffentlichen asymmetrischen Schlüssel des Empfängers [Jtk95].

Mit diesem Verfahren läßt sich nun die Authentizität einer Nachricht beweisen. Der Sender verschlüsselt ein Komprimat (Hash-Wert) der Nachricht mit seinem privaten Schlüssel und erzeugt damit eine digitale Signatur, die der Empfänger mit dem öffentlichen Schlüssel nachprüfen kann. Dies stellt sicher und beweist, daß der Sender der wirkliche Urheber der Nachricht ist und daß die Nachricht nicht verändert wurde, denn nur der Sender besitzt den privaten oder geheimen Schlüssel, mit dem die digitale Signatur erzeugt wurde. Um die Verifikation einer digitalen Signatur zu prüfen, d.h. ob der angewandte öffentliche Schlüssel auch von dem behaupteten Sender stammt, muß auf eine dritte Instanz, die beide Kommunikationspartner verbindet, vertraut werden. Die dritte Instanz signiert ihrerseits mit ihrem geheimen Schlüssel die Zuordnung zwischen einem Namen und einem öffentlichen Schlüssel. Diese signierte Zuordnung wird auch als Zertifikat bezeichnet. Die Richtigkeit des

Zertifikats läßt sich mit dem öffentlichen Schlüssel der Zertifizierungsinstanz nachprüfen. Auf diese Weise entsteht ein Netzwerk von Zertifizierungsinstanzen, das dezentral organisiert und betrieben werden kann und das die Basis der Authentizitätsbeweise der Benutzer bildet. In der Praxis existiert noch keine globale Zertifizierungsinfrastruktur. Es gibt nur wenige lokale Zertifizierungsinstanzen, die auf experimenteller Basis arbeiten. In den USA werden die mit der Schlüsselablage beauftragten Zertifizierungsinstanzen nach kontroverser öffentlicher Diskussion voraussichtlich nicht in staatlicher Hoheit verwaltet werden. Ein Kompromißvorschlag sieht vor, die Schlüssel bei Banken oder Versicherungen als dritte Instanz zu hinterlegen [VDI96 6].

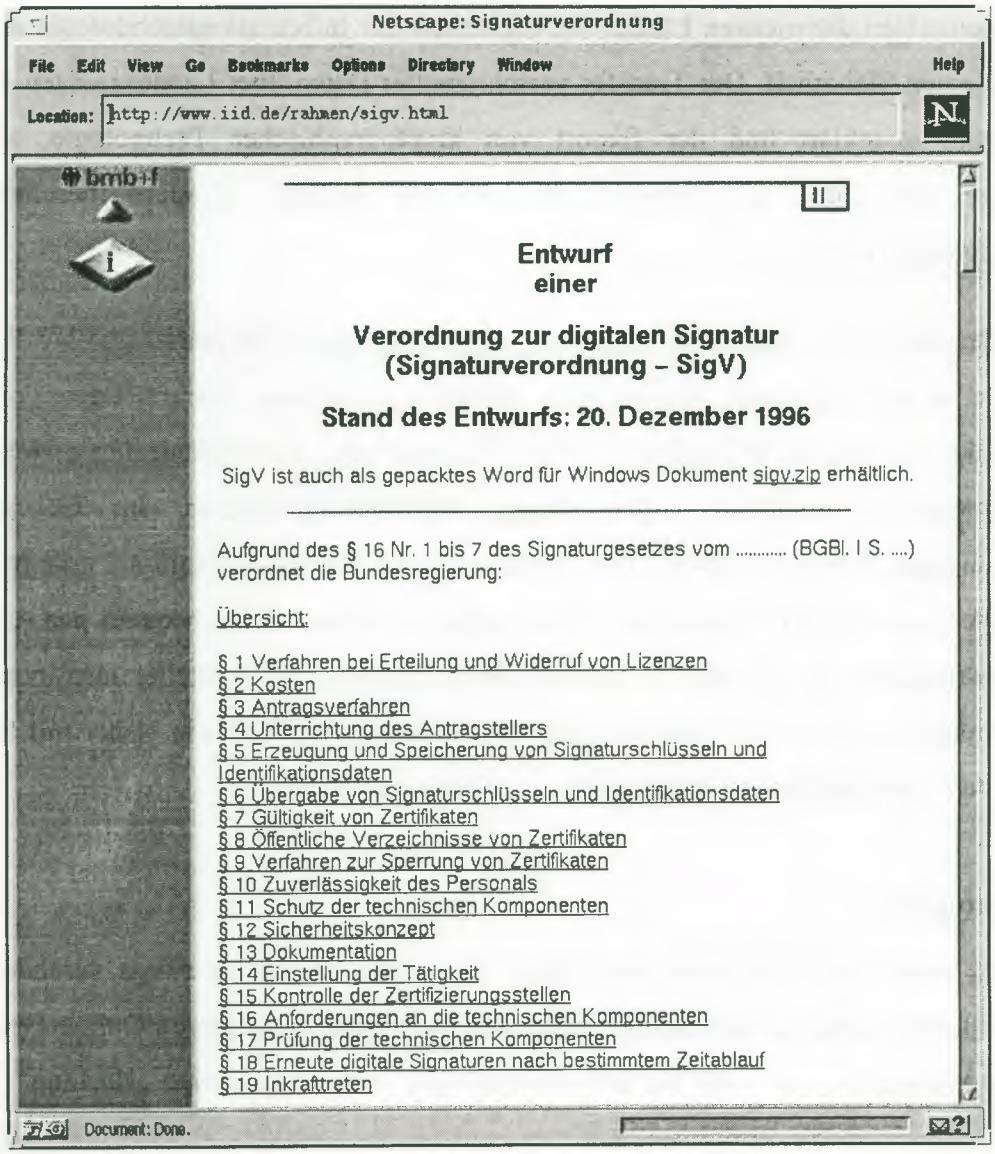

Abbildung 1: Entwurf Signaturverordnung BMBF

Eine routinemäßige Anwendung dieser Technologie erfordert aber auch, daß sie in die Endanwendungen, beispielsweise in die Mailsysteme oder in die WWW Clients und Server eingebaut ist, damit die Erzeugung und Verifikation digitaler Signaturen automatisch erfolgen kann. Es gibt aber bisher keine Produkte mit dieser Technologie, da die dazu notwendige Zertifizierungsinfrastruktur nicht existiert. Es ist aber damit zu rechnen, daß sich die flächendeckende und anwendungsübergreifende Nutzung von zertifizierter „Public-Key-Technologie" entwickeln wird.

Verfahren wie DES und RSA gelten vom kryptographischen Standpunkt als sicher, d.h. unbrechbar, wenn mit entsprechend großen Schlüssellängen gearbeitet wird. Aus diesem Grund betrachten die meisten Länder die Sicherheit der Informationstechnologie als Bereich der nationalen Sicherheit. Der Transfer verschlüsselter Daten über Landesgrenzen hinweg ist weitgehend ungeklärt und der Export von kryptographischer Technologie, sowohl in Hardware als auch in Software, ist in den meisten Ländern beschränkt und genehmigungspflichtig.

So ist das derzeit am weitesten verbreitete kryptographische Verfahren im WWW das von Netscape Communications Corporation entwickelte Secure Socket Layer (SSL) nur beschränkt zum Export freigegeben. Um eine Exportlizenz zu erhalten, durfte Netscape den Sitzungsschlüssel nicht in voller Länger chiffriert übertragen. Im Gegensatz zur amerikanischen Version (128-bit) war bisher lediglich ein 40-bit Schlüssel erlaubt. Auch in den USA ist die 40-bit Version des Clients sehr verbreitet, da sie bequem per Anonymous FTP downloadbar ist. Ab dem 1. Januar 1997 dürfen die US-Hersteller ihre internationale Kommunkation (Export von Softwarepaketen und Rechnern) statt wie bisher mit Schlüsseln von 40 bit Länge auf die Verschlüsselung von 56 bit aufrüsten[6].

2.2.4 Integrität

Der Weg einer Nachricht wird dahingehend überprüft, ob sie unterwegs verändert wurde. Besondere Bedeutung kommt der Integritätsprüfung bei der Aufgabe von Online-Bestellungen zu. Eine weitverbreitete Form der Integritätsprüfung ist das sogenannte „Hashing". Auf dem

---

[6] Angemessen wäre aber im Urteil von Fachleuten bei finanziellen Transaktionen Schlüssel mit einer Mindestlänge von 60 Bit. In den USA sind im inländischen Handel 128 bit verfügbar [VDI96].

Dokument wird eine Hashfunktion angewendet, die aus einer beliebig langen Nachricht eine Kurzerkennung generiert [Rei95]. Dieser Hashwert, der auch als Message Authentification Code oder Message Digest (MAC/MD) bezeichnet wird, verändert sich, wenn das Dokument bei der Übermittlung manipuliert wurde. So kann durch eine Berechnung des Hash-Wertes vor und nach dem Datentransfer und mittels Vergleich der beiden Werte auf Empfängerseite die Integrität der Daten überprüft werden.

2.2.5 Nicht-Rückweisbarkeit / Verbindlichkeit

Bei der Nicht-Rückweisbarkeit bzw. Verbindlichkeit wird geprüft, ob der in der Nachricht vermerkte Absender die Nachricht auch tatsächlich verfaßt hat. Dies ist insbesondere dann wichtig, wenn es im Rahmen eines vertragsrechtlichen Streits um die Frage geht, ob die abgegebene Willenserklärung auch wirklich von einer bestimmten Person getätigt wurde. Diese Verbindlichkeit bzw. Nichtabstreitbarkeit wird durch verschiedene Authentifizierungstechniken wie z. B. biometrische Verfahren oder durch digitale Signaturen sichergestellt. Sogenannte Zeitstempel erlauben darüber hinaus eine historische Nachweisführung. Wird jedem Transfer ein Zeitstempel zugeordnet, kann auch ein Wiederversenden derselben Nachricht von unbefugten Dritten, ein *Replay-Attack*, verhindert werden [Klu95].

2.2.6 Authentizität

Die Authentizitätsprüfung läßt sich unterteilen in die Authentifizierung der Informations- und Kommunikationstechnologie und in die Authentifizierung der beteiligten Kommunikationspartner. Die an einer Transaktion beteiligten Parteien müssen sich sicher sein, daß sie wirklich mit demjenigen kommunizieren, mit dem sie in Verbindung stehen wollen, was sowohl für den angeschlossenen Computer als auch für die Benutzer selbst gilt.

Übertragungsprotokolle zur Verschlüsselung von Daten über das World Wide Web (WWW) und der Email stellen die Authentizität der Informations- und Kommunikationstechnologie dar. Die Authentifizierung von Personen wird durch Lösungsansätze wie z. B. das Paßwort oder die digitale Signatur erzeugt.

2.3 Authentizität der Rechner über Protokollspezifikationen

Die Authentizität beteiligter Computer bzw. Rechner bei einer Online-Transaktion ist dann gewährleistet, wenn es sich wirklich um den Rechner mit entsprechender Adressierung handelt, als der er sich ausgibt. Erkennungszeichen sind die IP-Adressen, die jedem vernetzten Computer eindeutig zugeordnet werden können. Um die Authentizität zu gewährleisten, sind verschiedene Übertragungsprotokolle entwickelt worden, die durch die Web-Browser zur Verfügung gestellt werden. Die nachfolgend beschriebenen Sicherheitsschemata bilden die Grundlagen für sichere elektronische Zahlungen im WWW und sorgen für die Authentizität der kommunizierenden Rechner (Server und Clients).

2.3.1 Basic Authentification

Die praktische Implementierung von kryptographischer Technologie soll im weiteren am Beispiel der weitverbreiteten Applikation im Internet, dem WWW mit dem Übertragungsprotokoll HTTP dargestellt werden. Der Vorschlag für HTTP/1.0 definiert einen Mechanismus namens **Basic Authentication**, der praktisch standardmäßig in allen verfügbaren Browsern implementiert ist. Der Anwender besitzt ein Paßwort, das mit dem Nutzernamen stringverkettet und auf Anforderung base64-kodiert an den Server gesendet wird. Der Server überprüft, ob Benutzerkennung und Paßwort korrekt sind und sendet im Erfolgsfall die Nachricht. Auch wenn die Übertragung praktisch unverschlüsselt erfolgt, schützt dieser Mechanismus zumindest vor "zufälligem" unauthorisiertem Zugriff. [Reif95, Klu96)[7]. Ein Nachteil ist jedoch, daß Benutzerkennung und Paßwort unverschlüsselt und somit nicht vor dem Abhören geschützt übertragen werden können. Kauftransaktionen in Verbindung mit Kreditkartendaten sollten auf diesem Wege nicht übermittelt werden.

2.3.2 Secure Hypertext Transfer Protocol (S-HTTP)

Einer der ersten Ansätze wurde mit S-HTTP (Secure Hypertext Transfer Protocol), einer Erweiterung des HTTP-Protokolls von der Firma Terisa Systems, einer Joint Venture von RSA Data Security Inc. und EIT Enterprise Integration Technologies, entwickelt. S-HTTP stellt einen Rahmen für die Anwendung verschiedener kryptographischer Standardmethoden

[7] Der Vorschlag von Ari Luotonen stellt eine Erweiterung des Basic-Authentication-Mechanismus dar, die sich aber nicht durchsetzte [Reif 95].

dar. Jede Nachricht kann durch eine beliebige Kombination aus drei Mechanismen geschützt werden: Digitale Unterschrift (digital signature), Datenverschlüsselung und Authentifizierung. Eine S-HTTP-Nachricht besteht aus einer gekapselten HTTP-Nachricht und einigen vorangestellten Kopfzeilen, die das Format der gekapselten Daten beschreiben. Als Formate für die gekapselten Nachrichten werden bislang die Standards PGP, PEM, PKCS#7 (PEM ähnlich, von RSA DSI) unterstützt. Beide Seiten können im Rahmen einer Verhandlung Angaben über die verwendbaren bzw. geforderten Erweiterungen gegenüber HTTP machen. Dazu gehören: Nachrichtenformate, Typen der Zertifikate, Schlüsselaustauschmechanismus, Verfahren für digitale Unterschriften, Hash-Algorithmus für den Message Digest sowie Verschlüsselungsverfahren für Kopf und Inhalt. Der Client verschlüsselt z. B. alle Nachrichten mittels DES und vermag mit DES oder RC4-Algorithmen verschlüsselte Nachrichten zu empfangen.

S-HTTP definiert einen neuen URL-Protokolltyp "https", der auf die Fähigkeiten des Servers bezüglich S-HTTP hinweist. Der Client wird damit aufgefordert, bereits die Anforderungen gekapselt zu senden. Als primäre Webseite, auf der Produkte via S-HTTP bestellt werden können, darf CommerceNet gelten.

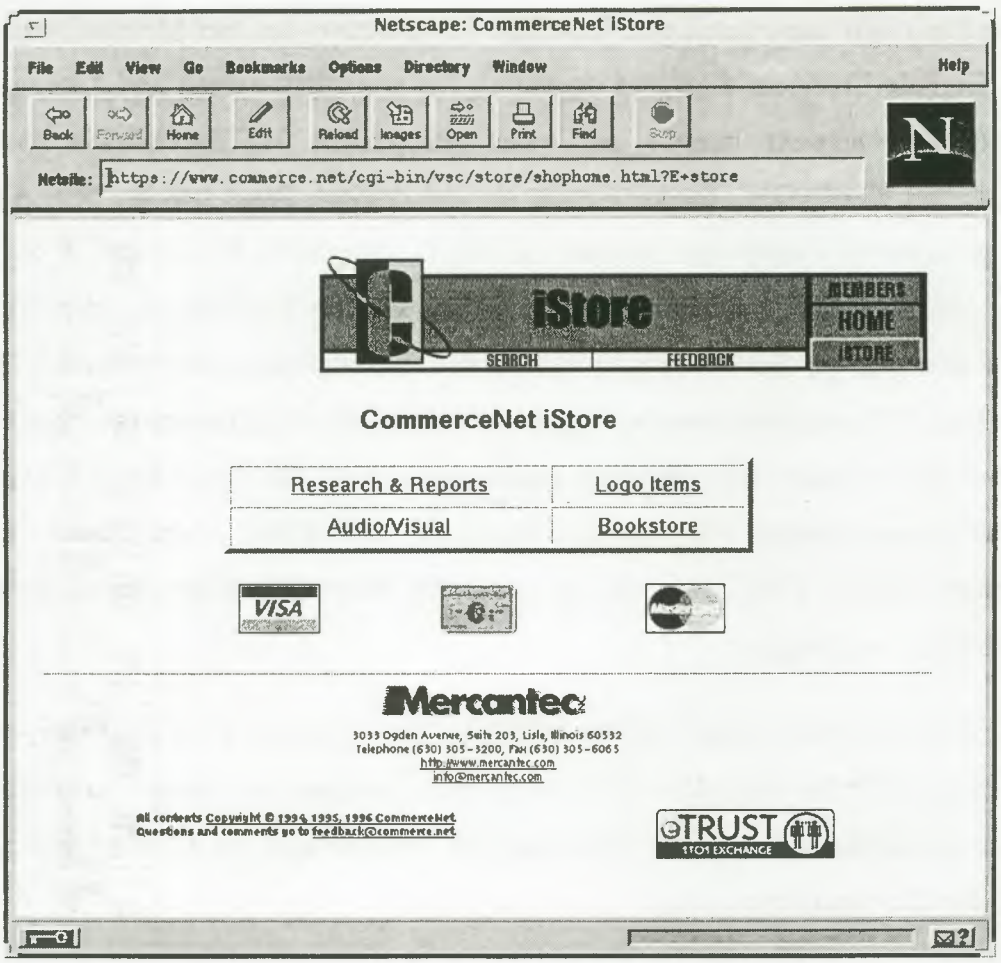

Abbildung 2: CommerceNet „iStore"-Eingangsseite.

Der ungebrochene Schlüssel am linken unteren Bildschirmrand, wie hier am Beispiel der CommerceNet-Website[8], symbolisiert die Verschlüsselungsübertagung mittels S-HTTP.

Die Entwickler des Protokolls haben Mosaic und NCSA-httpd modifiziert (Secure Mosaic, Secure-httpd) und stellen den Mitgliedern des CommerceNet-Konsortiums ein Toolkit für eigene S-HTTP-Implementierungen zur Verfügung. Verschiedene Firmen, darunter auch Netscape Communications, betreiben eine Integration des Protokolls in ihre Produkte.

2.3.3 Secure Socket Layer Protocol (SSL)

Das zweite Protokoll mit kommerziellem Hintergrund wurde bekannt und erlangte seine Bedeutung durch die große Verbreitung des Web-Browsers Netscape Navigator. Dieser Client

[8] http://www.commerce.net

beinhaltet ein sogenanntes Secure Socket Layer Protocol. Wie der Name andeutet, ist es nicht nur für HTTP vorgesehen, sondern soll jedes zuverlässige Transportprotokoll (im Falle Netscape/SSLRef:TCP) um ein Konzept für einen sicheren Kanal (Vertraulichkeit, Authentifikation, Datenintegrität) erweitern. SSL setzt auf die Socket-Schnittstelle auf, den Standard für den Zugriff auf TCP unter Unix und Windows, und ersetzt sie durch eine um die genannten Eigenschaften erweiterte Version. Dadurch wird eine neue Schicht zwischen dem Datentransportprotokoll TCP und den Anwendungsprotokollen wie HTTP, SMTP (Email) und FTP erzeugt. Daten des Web-Browsers werden erst von SSL verschlüsselt und gehen dann über TCP an den Empfänger und werden dort entschlüsselt. Damit stehen die neuen Sicherheitsmerkmale allen Anwendungsprotokollen (neben http auch FTP, Telnet etc.) zur Verfügung [Pfeffer96].

Vor der Übertragung der eigentlichen Daten arbeiten Client und Server ein "Handshake"-Protokoll ab, indem der Sitzungsschlüssel ausgetauscht und die Authentifikation vorgenommen wird. Der Client generiert einen neuen Master-Key des Servers verschlüsselt an diesen. Aus diesem Hauptschlüssel mit verbindungsbezogenen Daten werden mittels einer Hash-Funktion die Sitzungsschlüssel abgeleitet, die für die Datenverschlüsselung Anwendung finden. Für jede Richtung (Senden/Empfangen) wird dabei ein eigener Sitzungsschlüssel benutzt. Der Hauptschlüssel selbst kommt bei der Datenverschlüsselung nie zum Einsatz. Abschließend schickt der Client die mit seinem Sendeschlüssel chiffrierte Connection-ID und der Server den mit seinem Sendeschlüssel verschlüsselten Einmalwert. Der Client überprüft unter Verwendung seines Empfangsschlüssels, ob der Einmalwert mit dem von ihm gesendeten übereinstimmt und kann damit sicher gehen, daß der Server als der tatsächliche Inhaber des Zertifikats authentisch ist (andernfalls könnte der Server den Hauptschlüssel nicht korrekt entschlüsseln und folglich keine Sitzungsschlüssel generieren). Der Server hat ebenfalls die Möglichkeit die Authentifikation zu überprüfen. Zum Abschluß schickt der Server dem Client verschlüsselt, die Session ID. Nach erfolgreicher Beendigung des Handshake-Protokolls sind beide Seiten zur Übertragung der Anwendungsdaten bereit. Diese werden im Rahmen eines Record-Protokolls nach dem vereinbarten Verfahren verschlüsselt und mit einem Message Authentication Code zur Gewährleistung der Datenintegrität versehen. Sicherheitsbedenken an der SSL-Protokollverschlüsselung ergaben sich, als am 14. Juli 1995 Hal Finney einen Aufruf startete, um einen Sitzungsmitschnitt zwischen dem Netscape-Client und Netscape`s Secure Server zu knacken. Damien Doligez aus Frankreich war der erste, der einen Monat später die Lösung bekannt gab. Zuvor hatte ebenfalls eine

weitere Gruppe - unabhängig davon - mit vernetzten Workstations die Sitzungsschlüssel mit hoher Rechnerleistung herausfinden können.

Insgesamt bewertet gilt das SSL-Protokoll als ein sehr einfacher und effizienter Mechanismus zur Reduzierung des Sicherheitsrisikos vieler Anwendungsprotokolle. Vorteilhaft ist, daß es trotz der reduzierten Verschlüsselungsverfahren in Europa aufgrund des Netscape Navigators weit verbreitet ist und mehrere Anwendungsprotokolle unterstützt. Längerfristig werden in Publikationen auch Planungen angesprochen, die SSL und SHTTP zusammenführen wollen [Klu95].

2.3.4 Private Communication Technology (PCT)

In Anlehnung an Netscape`s Secure Socket Layer (SSL) Protocol versuchte Microsoft ein Konkurrenzprotokoll namens Private Communication Technology (PCT) einzuführen, das ebenfalls Funktionen zur Authentifizierung von Server und Client zur Verfügung stellt. Die ursprüngliche Zielsetzung für die Entwicklung von PCT von Microsoft war allerdings nicht einen offenen Standard zu implementieren, sondern bei einer späteren Einführung prozentual bei kommerziellen Geschäften mitzuverdienen. Das entwickelte Protokoll gilt als Derivat des SSL-Protokolls, das Sicherheitsschwachstellen von SSL korrigierend aufgreift und Verbesserungen anbietet. Es ist entwickelt worden, um die Privatsphäre zwischen zwei Kommunikationsapplikationen und die Authentizität zwischen Server und optional Client zu gewährleisten. PCT legt ähnlich dem SSL-Protokoll eine zusätzliche Schicht über die Socket-Ebene als Anwendung an. Der Vorteil liegt auch hier darin, daß es nicht allein auf HTTP als Übertragungsprotokoll beschränkt ist, sondern vielmehr jedes beliebige TCP-basierte höhere Protokoll (FTP, WAIS, Telnet etc.) bedienen kann.

Ein Vorteil von PCT liegt im Verschlüsselungsmechanismus, der beispielsweise aufgrund der Trennung von Authentifizierung und Verschlüsselung eine höhere Rate aufweist als die SSL-Begrenzung von 40-bit. Zusätzlich zu den Funktionen der Verschlüsselung und Authentifizierung wird die Integrität der Nachricht durch einen auf der Hash-Funktion basierenden Message Authentification Code (MAC) sichergestellt.

2.3.5 Secure Electronic Transaction (SET)

Aufgrund der Initiative der Großbanken und Kreditkartengesellschaften, die durch eine Vielzahl konkurrierender Systeme zusätzliche Kosten und Nachteile erwarteten, verständigten sich die Mitglieder des Konsortiums, bestehend aus Microsoft, Netscape, IBM, VISA, Mastercard, Deutsche Bank und American Express, auf einen gemeinsamen Protokoll-Standard. Die Entwicklung von SET (Secure Electronic Transaction) war am 1. Februar 1996 geboren und wird seitdem als der zukünftige Standard gesehen. Mit SET wurden zudem die Vorgängerprotokolle Secure Electronic Payment Protocol (SEPP) und Secure Electronic Payment Technology (STT) abgelöst.

Die erste Anwendungssoftware wird allerdings nach Auskunft des Konsortiums erst im Jahr 1997 erwartet. American Express empfiehlt daher seinen Kunden, beim Online-Shopping auf Netscape's SSL oder CyberCash (siehe Kap. 9.1) zurückzugreifen.

SET (Secure Electronic Transaction) verschlüsselt die Übermittlung von Daten mittels kryptographischer Verfahren und gewährleistet so die Vertraulichkeit von Informationen durch Nachrichtenverschlüsselung, authentifiziert die an der Transaktion beteiligten Parteien, einschließlich Kartenbesitzer und Händler, durch digitale Unterschriften und Zertifikate und beinhaltet Sicherheitsfunktionen für die Integrität der Zahlungsanweisungen durch digitale Unterschriften für die Bestelldaten der geordneten Güter und Dienstleistungen. Nach der SET-Spezifikation werden für die Teilnehmer jeweils 2 Schlüsselpaare benötigt, ein allgemeines Paar (key-exchange key) für die Verschlüsselung der Transaktionsdaten und ein Paar (signature-key) zur Generierung der digitalen Unterschrift. Jedes Paar besteht aus einem allgemeinen und einem privaten Teil. Zunächst wendet SET das asymmetrische Verfahren an, bei dem ein Schlüssel zur Verschlüsselung und ein anderer zur Entschlüsselung benötigt wird. Wird der öffentliche Schlüssel zur Verschlüsselung verwendet, so kann nur mit dem privaten Schlüssel die Nachricht entschlüsselt werden und umgekehrt. Wie bereits oben angesprochen, ist der öffentliche Schlüssel dem Sender und Empfänger bekannt, während der private Schlüssel nur dem Sender bekannt ist. Der allgemeine Schlüssel wird zur Chiffrierung der gesamten Nachricht verwendet, der Signaturschlüssel dagegen zur Erzeugung einer digitalen Unterschrift. Mittels einer Hashfunktion stellt der Empfänger die Authentizität der Sender und die Integrität der Daten fest [Set96].

2.3.6 PGP und PEM als Email-Sicherheitsprotokolle

Im Internet haben sich Public-Key-Verfahren wie **PGP** (Pretty Good Privacy) oder **PEM** (Privacy Enhancement for Electronic Mail) in der Email-Applikation durchgesetzt [Fox95]. Bereits 1991 wurde die erste PGP-Version von Philip Zimmermann veröffentlicht [Zi95]. PGP kombiniert die zur Zeit als beste Verschlüsselungsalgorithmen beurteilten Verfahren RSA und Idea (International Data Encryption Algorithm) und hat eine wachsende Verbreitung im Internet. PGP ermöglicht sowohl die Verschlüsselung von Email, die die Vertraulichkeit sichert, als auch digitale Signaturen. Diese ist eindeutig, weil nur dem Sender der private Schlüssel bekannt ist, zudem läßt sich der Text vor Manipulationen schützen. PGP erzeugt das Schlüsselpaar selbst. Die Wahl der Schlüssellängen ist variabel, gebräuchlich und ausreichend ist zur Zeit 1024 bit, aber auch 2048 bit sind möglich. Ganz wichtig beim Hinzufügen eines neuen Schlüssels ist, daß man den Schlüssel mittels der digitalen Unterschrift zertifizieren kann. Darüber hinaus läßt sich angeben, inwieweit man selber den Schlüsselzertifizierungen des jeweiligen Partners vertraut. Dabei sind vier Stufen von null bis zum absoluten Vertrauen (Stufe 4) möglich [Fox95].

Der Standard „Private Enhanced Mail“ (PEM) ergänzt ein Mail-System um die vier Sicherheitsdienste Vertraulichkeit, Integrität und Authentizität und Nichtabstreitbarkeit einer Nachricht [Sch95]. PEM spezifiziert zwei Nachrichtentypen: integritätsgeschützte, authentische Nachrichten (Typ MIC) und solche mit zusätzlichem verschlüsseltem Nachrichteninhalt (Typ encrypted). Die Berechnung und das Anhängen eines Message Integrity Check (MIC) sichert Datenintegrität und -authentizität. Ein symmetrisches Kryptoverfahren gewährleistet die Vertraulichkeit.

Die Verschlüsselung der Nachricht erfolgt durch einen zufällig generierten und nur einmal verwendeten Schlüssel mit einem symmetrischem Kodierverfahren. Der symmetrische Schlüssel wird mit dem öffentlichen Schlüssel asymmetrisch verschlüsselt und im Kopf der Nachricht mitgeschickt. Den zertifizierten öffentlichen Schlüssel des Kommunikationspartners kann der Sender bei einem öffentlichen Verzeichnis oder direkt vom Empfänger anfordern. Die Unverfälschtheit des Schlüssels kann er anhand der digitalen Signatur der Zertifizierungsinstanz überprüfen. Dann erfolgt die eigentliche Nachrichtenverschlüsselung [Fox95 S.187].

Beide Verfahren zur Authentifizierung des Anwenders der Email-Applikation können für elektronische Zahlungstransaktionen übertragen werden, wenn mit dem Austausch von Emails Bestellinformationen, Zahlungsmodalitäten, Kreditkarteninformationen etc. verwandt werden. PGP stellt einen pragmatischen Lösungsansatz dar, während PEM eine hoch komplexe Infrastruktur zur Zertifizierung benötigt.

2.3.7 Protokollspezifikationen und die Anordnung innerhalb des TCP/IP-Referenzmodells

Die bisher beschriebenen Protokollspezifikationen unterscheiden sich hinsichtlich des Ansatzes der Wirkungsweise auf den unterschiedlichen Ebenen (Netzwerk, Internet, Übertragung und Anwendung) des TCP/IP-Referenzmodells. Folgende Abbildung in Anlehnung an Bhimani [Bhi96] soll schematisch einen Überblick über die Ebene und des Ansatzes geben.

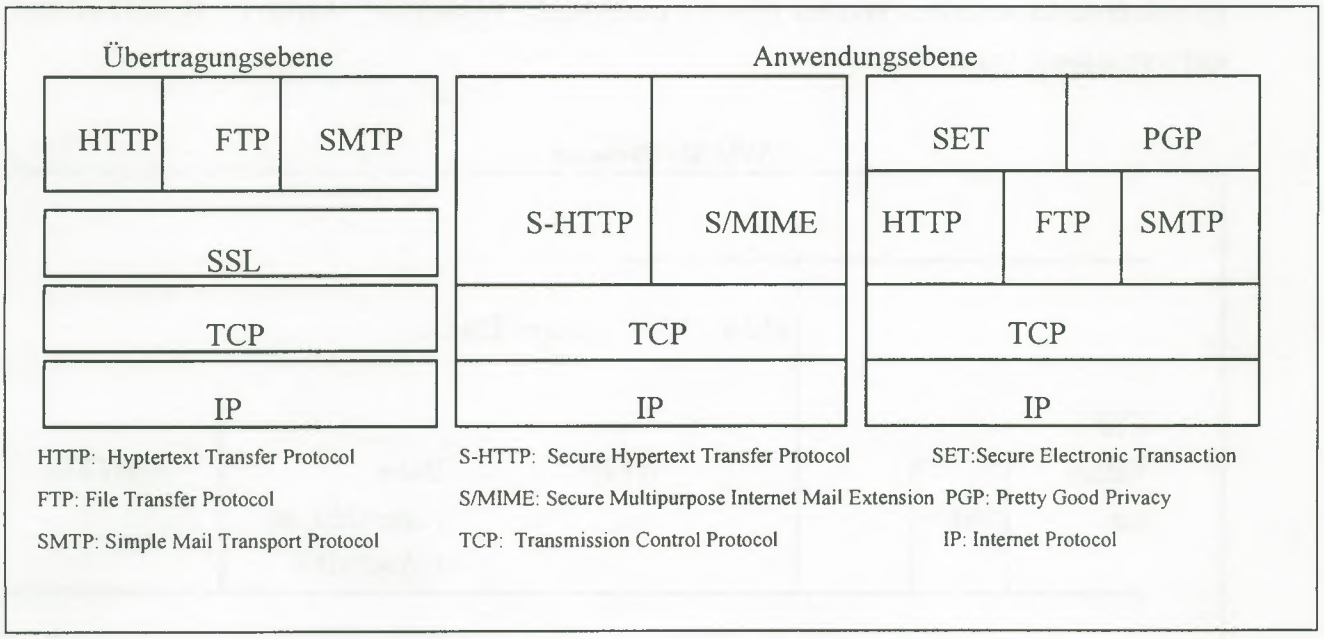

Abbildung 3: Anordnung von Sicherheitsansätzen im TCP/IP-Referenzmodells nach Bhimani

Die Internet Engineering Task Force (IETF) ist bestrebt, in den neuen Internet-Protokollen auf unterster Netzwerkebene sicherheitsrelevante Funktionen zur Überprüfung von Authentizität und Integrität über Verschlüsselungsverfahren zu implementieren. Das Internet-Protokoll in

der Version Ipv6 soll die Authentifizierung über die Hash-Funktion MD5 und den symmetrischen Schlüsselalgorithmus DES unterstützen.

SSL wird als Lösungsvorschlag zwischen dem TCP und der Sitzungsebene eingeschoben. HTTP, FTP und SMTP sind innerhalb spezifischer Anwendungsprotokolle definiert und weitere Protokollspezifikationen (SHTTP, SET, PCT, IKP) setzen auf bereits existierende Anwendungsprotokolle auf. Auf welcher Ebene die Sicherheitsproblematik letzten Endes am besten gelöst wird, ist unumstritten. Lösungsansätze auf unterer Ebene haben den Vorteil der Übersichtlichkeit, wirken akzeptanzerhöhend und können in Applikationen [Bhi96 S.31] umgesetzt werden, während Lösungsansätze auf hoher Anwendungsebene Speziallösungen darstellen, aber individuell auf bestimmte Anwendungen abgestimmt werden können.

2.3.8 Protokollspezifikationen aus der Sicht des WWW-Browsers

Da die vorgestellten Mechanismen an unterschiedlichen Stellen des TCP/IP-basierten Protokollstacks ansetzen, können sie auch miteinander kombiniert werden (z. B. SHTTP mit SSL) [Reif95 S.176].

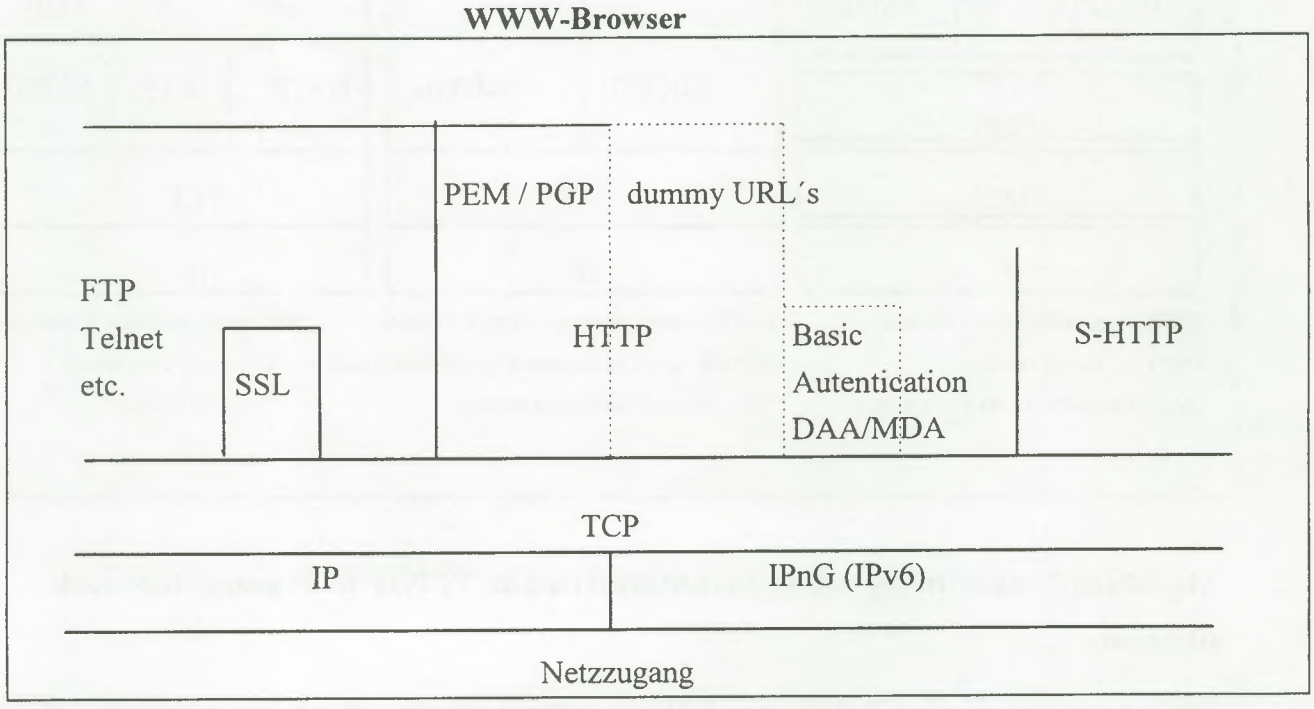

Abbildung 4: Ansatzpunkte sicherheitsrelevanter Lösungsansätze am TCP/IP-Protokollstack

2.4 Authentizität von Personen

Neben der Authentizität der Rechnerkonfiguration nimmt die Authentizitätsprüfung von Personen bei Online-Transaktionen eine zentrale Rolle ein, denn durch sie kann gewährleistet werden, daß der Zugang zu bestimmten Daten nur dann erlaubt wird, wenn der Anfragende nach einer eindeutigen Verifikation als berechtigter Nutzer des geschützten Systems erkannt wird. Die Authentizität von Personen überprüft die Identität der Kommunikationspartner am anderen Ende der Internetverbindung, um sicherzustellen, daß z. B. ein Kunde direkt mit seinem Zahlungsinstitut und nicht mit einer unbekannten dritten Partei kommuniziert. Ebenso kann auch das Institut oder ein Händler wiederum die Identität des Kunden verifizieren.

Eine einfache Form dieser Verifikation ist die Verwendung eines Paßwort-Schutzes in Verbindung mit einem User-Namen oder die Personal Identification Number (PIN). Verfahren zur Erzeugung digitaler Unterschriften erzeugen ebenfalls eine Authentizität. Häufig werden Authentizitätsprüfungen über Telefonleitungen (also Direktverbindungen zwischen Kunde und Anbieter) durchgeführt. Die verschiedenen Authentifizierungsmechanismen und Methoden, die in Applikationen Anwendung finden, sollen kurz skizziert werden.

2.4.1 Paßwort-Schutz

In Computernetzen ist das Paßwort das derzeit gängigste Authentifizierungsverfahren. Die sogenannte Persönliche Identifikationsnummer (PIN) ist ein Paßwort, das aus beliebigen Zeichen, Buchstaben oder Zahlen bestehen kann. Aus Sicherheitsgründen wird es oft in Verbindung mit einer zusätzlichen Karte verwendet (z. B. PIN und EC-Karte) oder in Verbindung mit einer einmaligen Transaktionsnummer (TAN). Durch die PIN/TAN-Kombination läßt sich jede Transaktion identifizieren und dem Benutzer zuordnen. Ein Replay-Attack wird dadurch unmöglich, da die TAN sofort nach der Verwendung ihre Gültigkeit verliert. Eine Verbesserung des Paßwort-Schutzes kann durch die Verwendung sogenannter Einmalpaßwörter erreicht werden, die nach dem Gebrauch sofort ungültig werden. Ausspionierte Paßwörter können somit nicht genutzt werden.

2.4.2 Verschlüsselung durch Kerberos

Kerberos ist ein Verschlüsselungsverfahren, das am Massachusetts Institute of Technology (MIT) entwickelt wurde. Kerberos ermöglicht die Identifikation von Benutzern in einem offenen, ungesicherten Netzwerk. Mögliche Störfaktoren wie das Abhören der Leitung, die

Benutzung falscher IP-Adressen (Spoofing) und die Störung der Kommunikation sollen durch Kerberos verhindert werden. Mittels kryptographischer Verfahren läßt sich eine individuenspezifische Authentifizierung unter Zuhilfenahme einer dritten Instanz verwirklichen [Bra96]. Die Authentifizierung erfolgt nach dem Login an einem an das Netz angeschlossenen Computer. Die dritte Instanz ist verantwortlich für die Schlüsselverteilung, dem sogenannten „Key Distribution Service" (KDS). Jeder Teilnehmer besitzt einen gemeinsamen symmetrischen Schlüssel mit dem KDS, der bei jeder Übermittlung zwischengeschaltet ist. Der Sender schickt eine mit seinem geheimen Schlüssel chiffrierte Nachricht an den KDS und gibt den Empfänger an. Der KDS entschlüsselt die Nachricht, chiffriert sie wieder mit dem geheimen Schlüssel des Empfängers und sendet sie an diesen weiter. Auf diese, etwas verkürzt dargestellte Funktionsbeschreibung basiert das Kerberssystem [Kon93].

2.4.3 Smartcard

Die Smartcard besitzt im Gegensatz zur Magnetkarte einen Mikroprozessor, der es ermöglicht Informationen zu speichern und zu verarbeiten. Die Karte beinhaltet ein eigenes kleines Betriebssystem verbunden mit Daten und einem Programm. Die Smartcards können über entsprechend Geräte gelesen werden (z. B. tragbare Leser), die an den PC angeschlossen werden können, oder über Leser im PCMCIA- oder Diskettenformat. Ist der Smartcard-Leser in die Hardware konfiguriert, kann die Smartcard alle bisher beschriebenen Authentifizierungsverfahren ausführen. So eignen sich Smartcards für die Berechnung von Einmalpaßwörter, zur Erzeugung digitaler Unterschriften, zur Speicherung von Schlüsselpaaren und zur Ausführung von kryptographischen Algorithmen [Hol95]. Für den elektronischen Zahlungsverkehr finden Smartcards neben den bereits beschriebenen Einsatzgebieten der Authentifizierung mittels digitaler Unterschriften für die Bereiche Electronic Cash (aufladbares Geld / Geldkarte) und Zahlungsautorisierung an Point-of-Sale-Automaten (POS) Verwendung [Hüb96, Str96].

In Konkurrenz zu den Kreditkartenorganisationen sind insbesondere die Banken an der Entwicklung vor allem der Smartcards interessiert, die die Magnetstreifenkarten ablösen sollen. Diese Smartcards können von entsprechenden Terminals mit Geld, das von den Banken stammen soll, aufgefüllt werden. Sie können die Authentifizierung ohne einen Server selbst durchführen und Transaktionen speichern, die dann als Beleg nachweisbar sind. Der

Vorteil liegt darin, daß bei Kauftransaktionen keine Rücksprache mit dem Kreditinstitut (Clearingstelle) erfolgen muß. Ein Beispiel für diese Umsetzung bietet das von der National Westminster Bank und der Midland Bank entwickelte MONDEX-Projekt (siehe Kap.4.3).

2.4.4 Hardware-Lösungsansätze

Zur Erhöhung der Sicherheit werden Hardware-Lösungsansätze entwickelt, die in Zusammenhang mit dem Personal Computer die für eine Transaktion nötigen Dienste, z. B. Schlüsselgenerierung, Verwaltung, Nachrichtenverschlüsselung, übernehmen. Häufig wird hierzu ein Chip als PC-Karte angeschlossen (z. B. PCMCIA-Steckplatz, ISA-Steckkarte). Zusätzlich berechnet dieser Chip einen Hashwert über die Nachricht, der die Datenintegrität garantiert und aus dem eine digitale Signatur generiert werden kann. Die Sparda Bank[9] setzt auf diese hardwarebasierte Lösung in ihrem Online-Banking. Der von der Leipziger Firma ESD[10] GmbH entwickelte „Me-Chip" ist über einen Parallelport mit der Tastatur verbunden und bietet damit keine Angriffspunkte für Manipulationen über das Netz. Allerdings werden diesen hardwarebasierten Sicherheitsysteme von Experten kaum noch Chancen eingeräumt, da sie noch weitgehend nicht standardisiert sind. Neben der kostenintensiven Hardware kann der Nutzer in Abhängigkeit geraten und nur die entsprechenden Stellen (Anbieter/Hersteller) nutzen, die diese Systemlösung unterstützen. Die Sparda Bank in Hamburg hat mit dem Me-Chip in Verbindung mit der Tastatur einen Online-Lösungsvorschlag basierend auf dieser Hardware-Lösung eingeführt.

2.4.5 Digitale Signatur

Die digitale Signatur als Authentifizierungsinstrument soll in Anlehnung an die herkömmliche Unterschrift den Unterzeichner eindeutig zuordnen, damit kein Zweiter oder Dritter diese Unterschrift wiederholen kann. Digitale Unterschriften basieren auf den bereits vorgestellten asymmetrischen Kryptographiealgorithmen. Zunächst wird das Dokument zur Gewährleistung der Vertraulichkeit vom Absender chiffriert (mit dem öffentlichen Schlüssel des Empfängers). Der Empfänger dechiffriert das Dokument mit seinem privaten Schlüssel (private key). Im Anhang des Dokuments befindet sich ein sogenannter Hash-Wert der auch als Message Digest

---

[9] http://www.sparda-hh.de

[10] http://www.esd.de

oder Message Authentication Code bezeichnet wird und mittels einer Hash-Funktion zuvor vom Absender erzeugt wurde. Um auch hier die Vertraulichkeit zu sichern, muß der Hash-Wert mit dem privaten Schlüssel des Absenders chiffriert werden. Der Empfänger des Hash-Wertes im Anhang muß diesen mit dem öffentlichen Schlüssel des Absenders dechiffrieren und kann anschließend den Wert vergleichen mit der Neuberechnung aus der Nachricht. Wenn das Ergebnis mit dem gesendeten Hashwert übereinstimmt, gilt die Nachricht als unverändert.

3. Elektronische Zahlungssysteme im Überblick

Um das Internet für kommerzielle Zielgruppen zu öffnen, bedarf es der Entwicklung von Techniken, die es erlauben, neben der Online-Bestellung und -Verrechnung per Nachnahme auch über das Internet direkte Zahlungen vornehmen zu können. Inzwischen gibt es eine Anzahl verschiedener Systeme für elektronische Zahlungen, die auf dem Internet teilweise optional betrieben werden. Die Spannbreite der verschiedenen Ansätze im Zahlungsverkehr reichen dabei von EDI-Transaktionen[11] bis zu den sogenannten Kleinstzahlungen (Micropayments). Die Bandbreite der Abbildung von Lösungsansätze für elektronische Zahlungssysteme ist äquivalent mit den Ansätzen in der realen Welt. So wird beispielsweise versucht, den Zahlungsverkehr mittels Bargeld, Eurocheque, Verrechnungsscheck und Kreditkarte im Internet abzubilden. Neben der Klassifizierung nach der Zahlungsgröße können weitere Kriterien zur Unterscheidung der elektronischen Zahlungsmethoden z. B.nach Online/Offline-, Pre-Paid/Post-Paid- und Anonymous/Non-anonymous-Systeme vorgenommen werden. Ohne im Detail auf die verschiedenen Methoden an dieser Stelle einzugehen, soll im wesentlichen die Klassifikation kurz vorgestellt werden.

3.1 Online / Offline Systeme

Online Systeme schalten beim Geldtransfer eine dritte Partei ein, die die Authentizität der Transaktion und deren Vollzug bestätigt, z. B. bei der Zahlung mit Kreditkarte, bei der ein sogenannter "Acquirer" neben Käufer und Händler mit einem Kreditkartenunternehmen als Dritter in Verbindung steht.

Bei Offline Systemen wird von der elektronischen Transaktion herkömmliches Geld in elektronisches gewechselt und auf einer speziellen Hardware (Chipkarte, Smartcard oder elektronische Brieftasche) gespeichert, die gegen physische und elektronische Manipulation weitgehend geschützt ist.

3.2 Pre-Paid / Post-Paid

Hier wird nach der zeitlichen Reihenfolge der Zahlung unterschieden. Da bei Offline Systemen zuvor der Umtausch von Geld in elektronisches Geld oder virtuelles Geld (Token,

---

[11] Die Begriffsdefinition und Darstellung von EDI erfolgt in Kap. 8

Cyberbuck, Cybermoney, Electronic Cash etc.) erfolgen muß, können wir Offline Systeme auch als Pre-Paid-Systeme klassifizieren. Online-Systeme, die Kreditkarteninformationen abfragen und bei denen zeitlich die Abbuchung i.d.R. nach der Lieferung erfolgt, können dagegen als Post-Paid Systeme kategorisiert werden.

3.3 Anonymous / Non-Anonymous

Eine wesentliche Eigenschaft herkömmlichen Geldes ist die Möglichkeit des anonymen Zahlungsverkehrs. Nach einem Transfer sind die Herkunft des Geldes oder die Zusammenhänge der Transaktion aus seiner Existenz nicht mehr herleitbar. Dies wird versucht bei elektronischen Verfahren mittels starker kryptographischer Algorithmen, spezieller Protokolle und sogenannter "blinder Unterschriften" nachzubilden.

System	Payment Model	Security	Anonymity
Online Systems:			
First Virtual by Mastercard / VISA http://www.fv.com	Post-Paid Credit Card based	No Cryptography	non-anonymous
Internet Shopping Network http://www.korner.nm.kr/shop.shop.	Post-Paid Credit Card based html	No Cryptography	non-anonymous
Ecash by DigiCash http://www.digicash.com	Pre-Paid Token based	Public Key Cryptography (RSA)	anonymous (blind signature)
iKP by IBM http://www.zurich.ibm.com	Post-Paid Credit Card based	Public Key Cryptography (RSA)	non-anonymous
NetBill by Carneie Mellon Univ. http://www.ini.cmu.edu/netbill/	Post-Paid or Pre-Paid	Shared-Key Cryptography (Kerberos / DES)	non-anonymous
NetCheque by the Univ. of South.California http://gost.isi.edu/gost-group/produ	Post-Paid Cheque based cts/netcheque/netcheque	Shared-key Cryptography (Kerberos / DES)	non-anonymous
NetCash by the Univ. of South.California http://gost.isi.edu/gost-group/produ	Pre-Paid token based cts/netcash/netcash	Public-Key and Shared-Key	non-anonymous
CyberCash by CyberCash http://www.cybercash.com	Post-Paid Credit Card based	Public Key Cryptography (RSA)	non-anonymous
Anonymous Credit Card by AT&T Bell Labs http://www.research.att.com/projects	Post-Paid Credit Card based	Public Key Cryptography	anonymous (pseudo)
Netcash by Software Agents, Inc.	Pre-paid token based	Public key Cryptography (PGP)	non-anonymous
Offline Systems:			
DigiCash "CAFE" ESPRIT Project http://www.cwi.nl/cwi/projects/cafe/	Pre-Paid Electronic Purse	Public key Cryptography	anonymous (blind signature)
Mondex (Smartcard) http://www.mondex.com	Pre-Paid Electronic Purse	No Cryptography Digital Signatures	non-anonymous

Abbildung 5: Kurzüberblick der verfügbaren Zahlungsysteme.

4. Elektronisches Geld

4.1 DigiCash (Ecash)

Einer der ersten Ansätze zur Verwirklichung eines anonymen, auf „Bargeld“ basierenden Systems wurde von der Firma DigiCash[12] entwickelt.

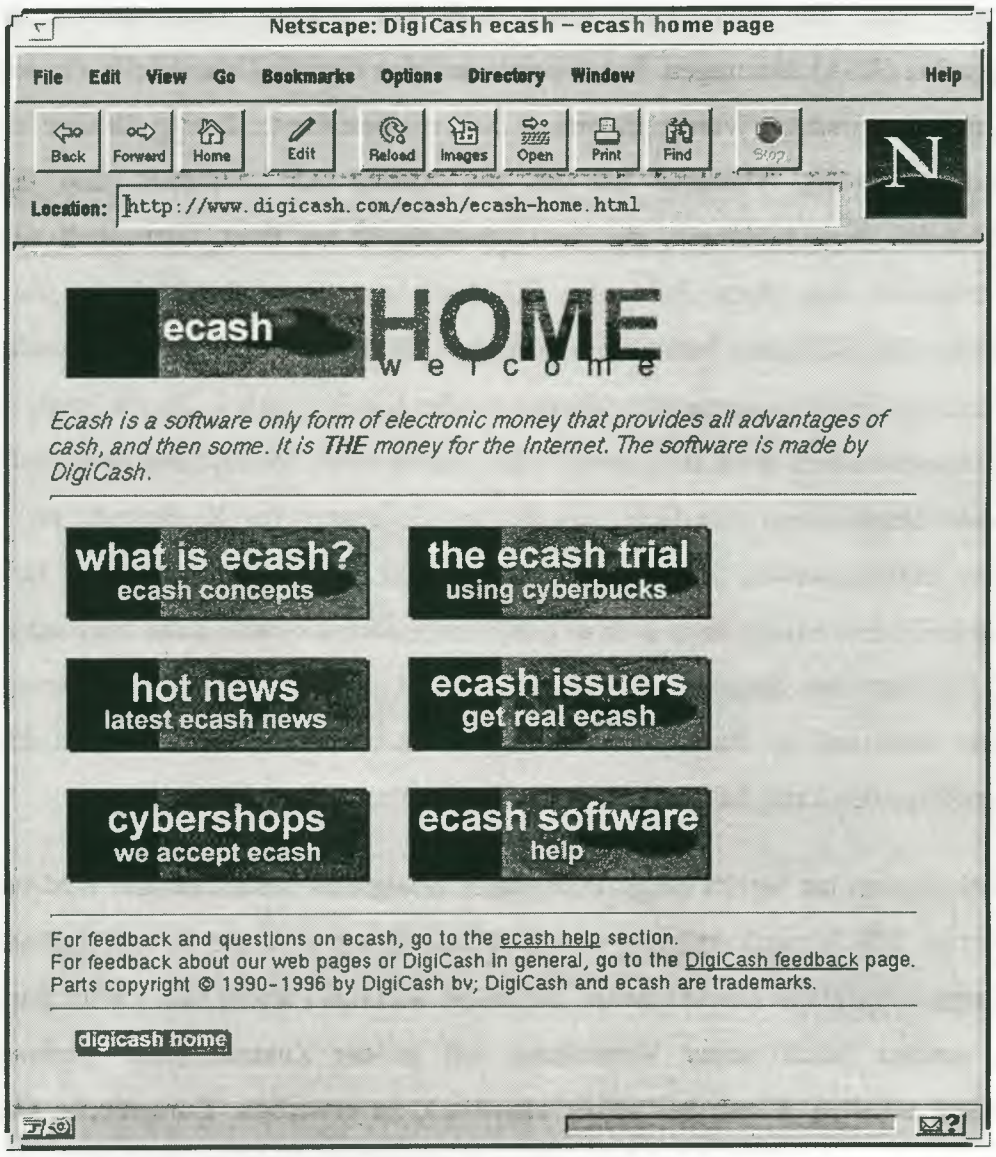

Abbildung 6: Informationsseite zu Ecash von DigiCash

Die Vorteile dieses Ansatzes sind, daß Kaufgewohnheiten, Präferenzen und Namen nicht erfaßt werden und der Zahlungsverkehr mit Bargeld im Bereich „low-payment“ bis

[12] http://www.digicash.com

„Millicent“ (Pfennigbeträge) abgedeckt werden kann. Ecash ist eine Technologie, die 1995 mit einem Preis der Europäischen Kommission, dem Information Technology European Award (ITEA) ausgezeichnet wurde.

Um Ecash zu benutzen, benötigt der Käufer ein Programm, damit vom Server der Bank ein bestimmter Betrag abgehoben werden kann, der dann lokal auf dem PC (Festplatte) gespeichert wird. Bei Kauftransaktionen wird das digitale Geld mittels Public-key-Kryptographie (RSA) übertragen. Ecash beinhaltet eine digitale Unterschrift, die analog einer Münze einen bestimmten Wert repräsentiert. Soll ein bestimmter Betrag für eine Transaktion bereitgestellt werden, berechnet der PC die Anzahl der „Münzen“ und erzeugt die entsprechenden Seriennummern, die dann verschlüsselt zur Bank übermittelt werden. Die Bank verwendet nun ihren Public-key-Schlüssel und verschlüsselt damit die Münzen, wodurch sie ihre Gültigkeit bekommen. Nachdem die Bank das Konto des Kunden belastet hat, schickt sie die gültig gemachten Münzen an den Kunden zurück. Da die Bank nicht weiß, welche Seriennummern der Kunde gewählt hat, hat sie keine Möglichkeit festzustellen, wofür der Kunde anschließend das Geld ausgibt. Im Gegensatz zur Kreditkarte ist Ecash ein anonymes Zahlungsmittel, analog dem realen Geld. Wenn ein Anwender Ecash durch Einkäufe in Umlauf bringt, kann es über den Stempelabdruck einer Bank zugeordnet werden, die die Echtheit des Stempelaufdrucks und damit auch der Münze verifiziert. Da der öffentliche Schlüssel der Bank jedem zugänglich ist und damit die Gültigkeit der Münzen nachgeprüft werden kann, ist eine Fälschung der Münzen ausgeschlossen.

Das Ecash-System hat bereits einige Pilotphasen erfolgreich bestanden und wird von einigen Anbietern im WWW zur Verfügung gestellt. Hinter Ecash steht die Firma DigiCash und der Kryptographie-Spezialist David Chaum, der einige wichtige Patente hält, die im Bankgewerbe genutzt werden. Nach seiner Vorstellung soll in der Zukunft jeder Verbraucher die Möglichkeit erhalten, Ecash bei seiner Hausbank zu erwerben. Europäische Großbanken haben bereits ihr Interesse am Ecash-System bekundet, auch wenn mitunter kritische Äußerungen von seiten der Banken und Regierungen zu hören ist, denn die Möglichkeiten des Mißbrauchs (Gelddruck, Geldwäsche etc.) ist noch nicht ausreichend evaluiert. Ecash befindet sich, neben den erwähnten Feldversuchen, unter dem Namen Cyberbucks auch in einer öffentlich zugänglichen Betaphase. Insgesamt akzeptieren bereits etwa 100 Web-Sites Cyberbucks. Darunter befindet sich auch die Deutsche Bank AG, die Ende letzten Jahres (1996) mit einer 6monatigen Pilotphase Ecash testet. Neben der Softwareinstallation auf dem

PC und einem Girokonto bei der Bank muß zusätzlich ein Ecash-Depotkonto eingerichtet werden. Von diesem Depotkonto können max. 400,- DM als Höchstbetrag auf die „Geldbörse“ des PC`s heruntergeladen werden. Die elektronischen Münzen müssen nicht permanent auf dem PC gespeichert werden. Sie können auch aus Sicherheitsgründen problemlos in das persönliche Ecash-Depot auf dem Rechner der Bank zurücktransferiert und nach Bedarf heruntergeladen werden.

4.2 Millicent (Electronic Microcommerce)

Das Ziel des Millicent-Ansatzes[13] ist es, ein möglichst preiswertes im Sinne eines „billigen“ Transaktionssystems für Kleinkunden zu schaffen. Auch Pfennigbeträge sollen damit kostendeckend transferiert werden können. Auf die Nutzung aufwendiger kryptographischer Verfahren kann dabei verzichtet werden, da die Kosten des „Einbruchs“ oder „Abhörens“ in der Regel größer sind als der Gewinnzuwachs.

Die Architektur basiert auf der Einführung einer dritten Instanz, dem sogenannten Broker zum Verkäufer bzw. Käufer. Käufer und Anbieter müssen bei ihm ein Konto eröffnen und erwerben sogenannte Scrips, d.h. Wertzertifikate mit Pfennigbereich bis zu DM 100, die auf dem PC gespeichert werden. Die erstmalige Einrichtung von Konten beim Broker werden mit kryptographischen Schlüsseln oder „offline“ via Telefon vorgenommen. Durch eine Art digitale Signatur (Zero Knowledge Proof) sind die Scrips vor Manipulation geschützt, so daß der Kunde seine Bilanz nicht verändern kann. Ist ein Broker kriminell, fällt dies den Händlern relativ schnell auf, wenn sie ungültige Scrips erhalten. Im umgekehrten Fall (Händler ist kriminell) werden Beschwerden bei dem Broker eingehen, der den Händler aus seiner Liste entfernen kann. Die nachfolgenden Abbildungen illustriert den Zahlungsprozeß aus der Sicht der beteiligten Parteien (Broker, Händler und Käufer).

[13] http://www.research.digital.com/SRC/millicent

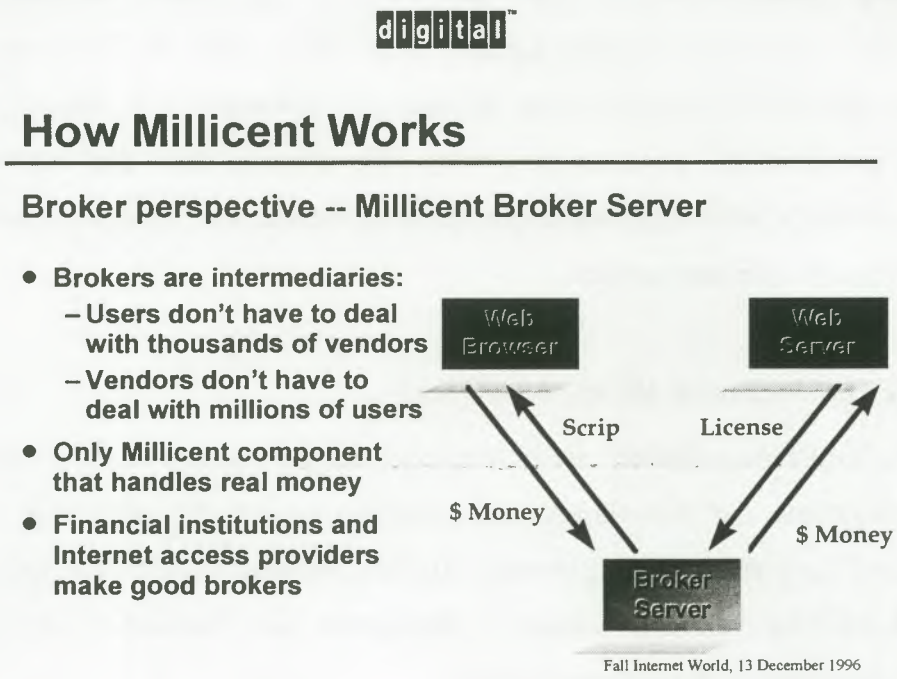

Abbildung 7: Funktionsweise des Millicent Broker Servers

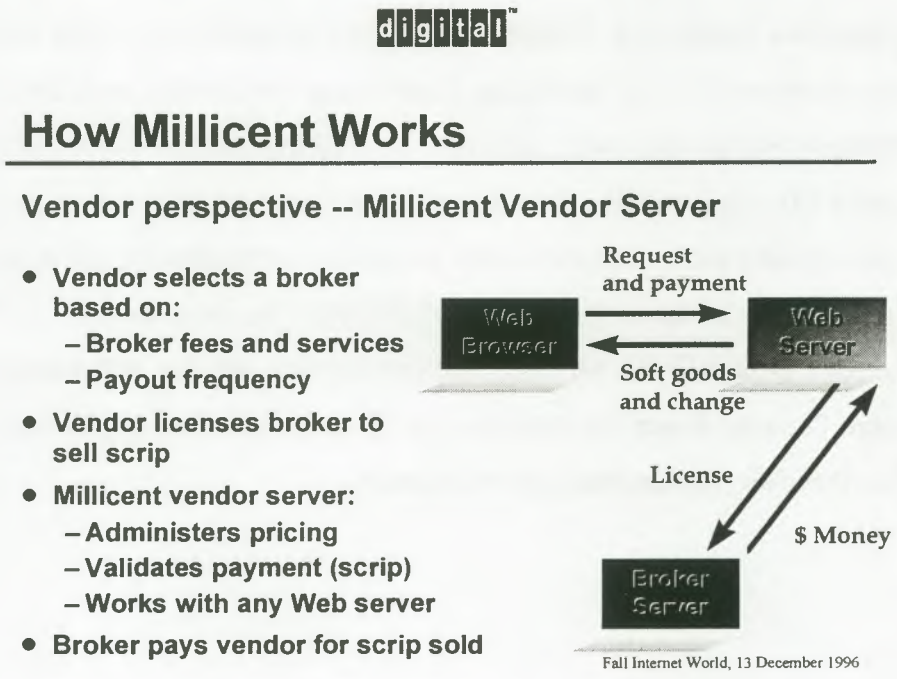

Abbildung 8: Funktionsweise des Vendor Servers

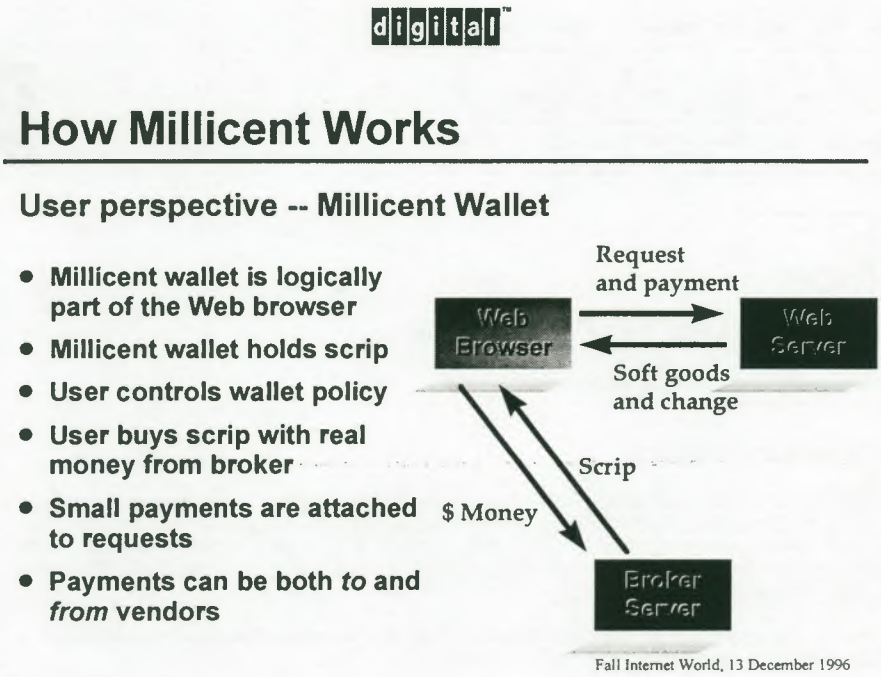

Abbildung 9: Funktionsweise des Millicent Wallets

4.3 Smartcard-Konzepte

Bei dem Smartcard-Konzept werden ähnlich dem Ecash-Prinzip Geldwerte auf einer Chipkarte digital gespeichert und mittels digitaler Signaturen implementiert. Beim Einkauf oder bei Transaktionen mit der Bank übernimmt der Chip auf der Smartcard die Erzeugung der digitalen Signaturen und die Überprüfung der Echtheit des Geldes. Ein internationales Forschungsprojekt, das die europäische Gemeinschaft finanziert, trägt den Namen CAFE (Conditional Access for Europe).[14] Das zentrale Ziel des CAFE-Projekts ist die Entwicklung eines sicheren elektronischen Zahlungssystems unter Wahrung der Anonymität und der Privatsphäre des Endkunden. Eines der diversen Zahlungsmittel im CAFE-Szenario soll von der Firma DigiCash gestellt werden.

[14] http://www.cwi.nl/cwi/projects/cafe.html

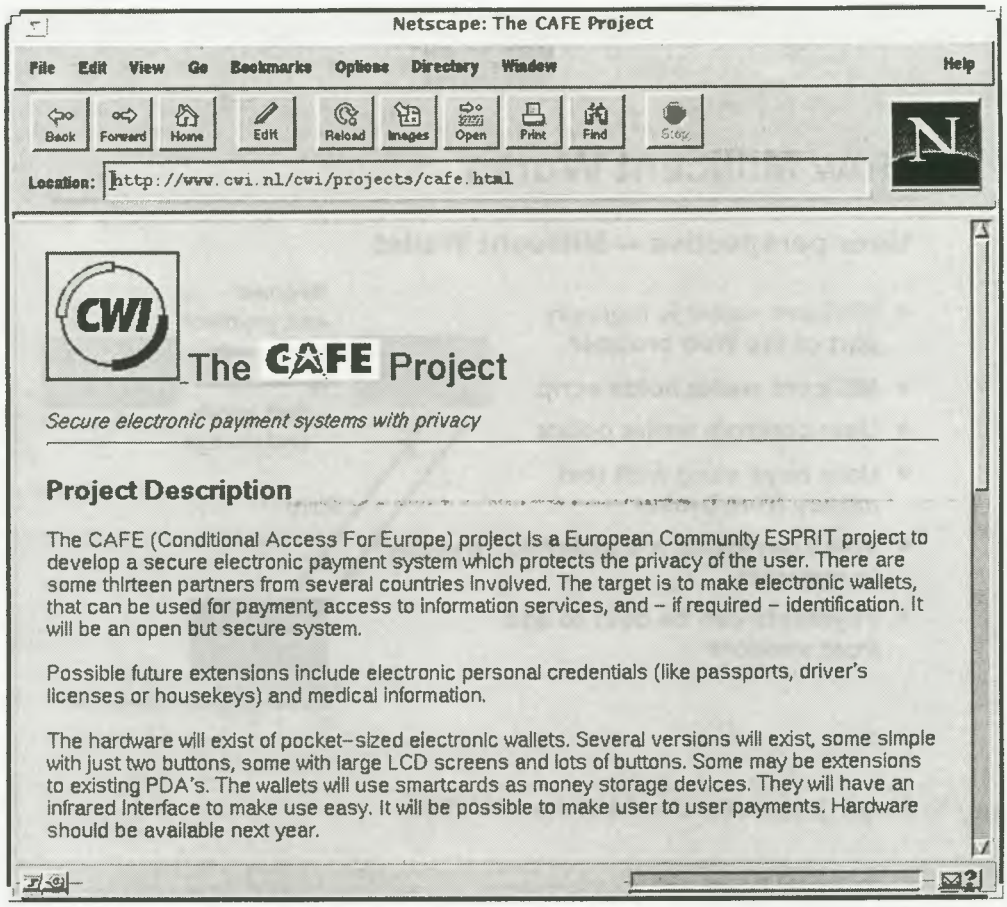

Abbildung 10: Homepage des CAFE-Projektes

Ein Beispiel für diese Umsetzung bietet das von der National Westminster Bank und der Midland Bank entwickelte MONDEX-Project[15] (Mondex Electronic Purse Programm). Bei einem Pilotprojekt im englischen Whiltshire wird der Smartcard-Ansatz im großen Stil getestet; kleinere Versuchsabläufe gibt es in Dänemark und Atlanta. Um die Interoperatibilität zwischen Smartcards und PC`s zu erhöhen, haben sich eine Interessensgemeinschaft aus Industrieunternehmen des Hard- und Softwarebereichs zusammengeschlossen, um Spezifikationen für die Bereiche Banking, Electronic Commerce, Health Care und Corporate Security zu erschließen. Zu dem Verbund gehören die Firmen Siemens Nixdorf[16], Hewlett Packard[17], Microsoft[18], Bull CPB[19] und Schlumberger Ltd.[20]. Das Ziel gilt der Entwicklung

[15] http://www.mondex.com

[16] http://www.siemens.de

[17] http://www.hp.com

[18] http://www.microsoft.com

eines internationalen Standards für elektronische Transaktionen basierend auf der Smartcard [Mit96].

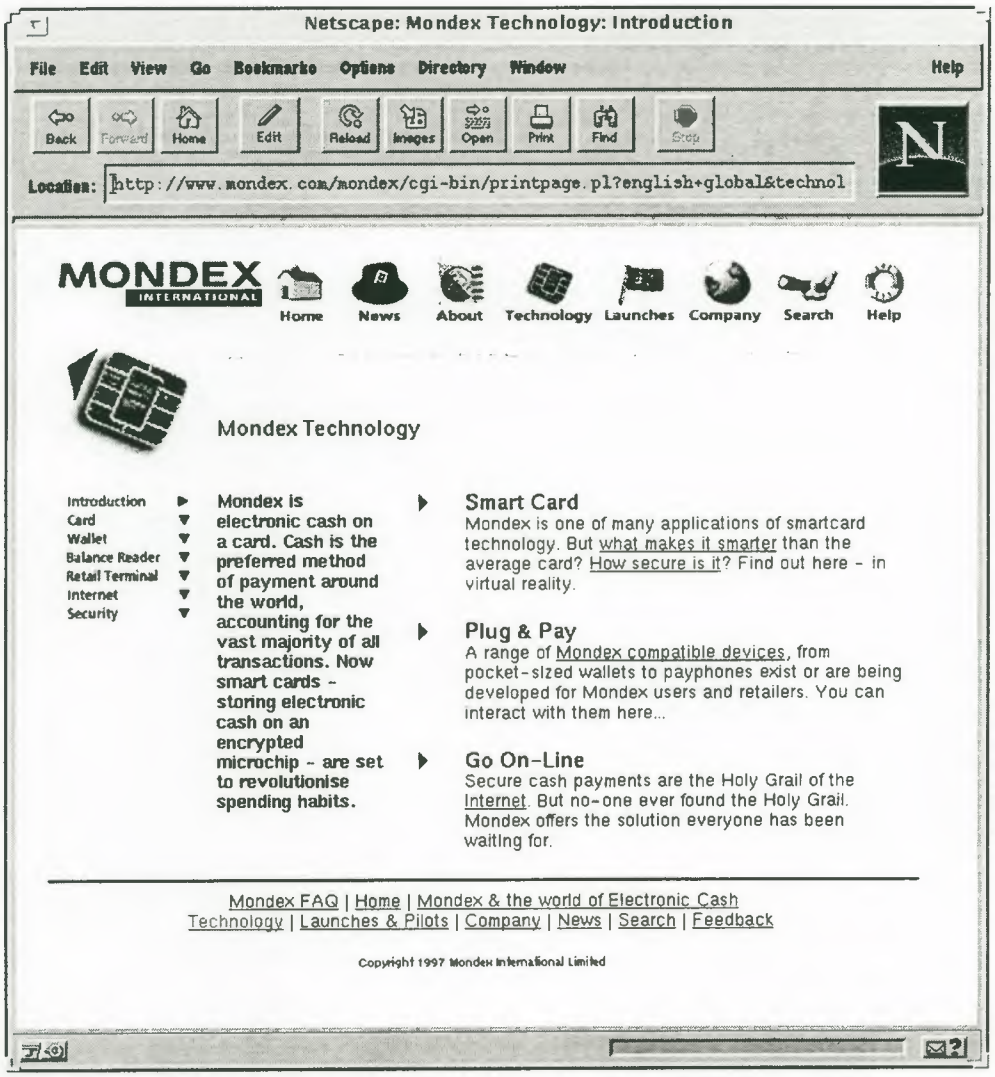

Abbildung 11: Einer der führenden Vertreter für Zahlungssysteme basierend auf der Smartcard ist die Firma Mondex.

In Deutschland wird in diesen Monaten die Geldkarte, eine Variante der Smartcard, von Banken und Sparkassen eingeführt. Sie kann bis zum Betrag von 400,- DM an bankeigenen Terminals aufgeladen werden und soll den Kunden im täglichen Einkauf als elektronische

[19] http://www.bull.com

[20] http://www.schlumberger.com

Geldbörse dienen [Hüb96]. Bis heute ist die Geldbörse aber noch nicht für Online-Transaktionen z. B. über Lesegeräte am PC vorbereitet.

5. Elektronische Scheck-Systeme

5.1 Netbill

Bei dem von der Carnegie-Mellon-University entwickelten Netbill[21] handelt es sich um eine Architektur, die auf dem herkömmlichen Scheckkonzept basiert. Der Kunde hat ein elektronisches Scheckbuch in der Form eines Client-Programms. Mit diesem Programm wird die ganze Transaktion abgewickelt, nachdem zuvor eine Preisangabe vom Händler erfolgte. Der Anbieter verfügt über ein Programm, das als „Registrierkasse" dient. Die Anfrage an den Händler wird über ein sicheres Protokoll abgewickelt, das die Identität des Käufers sicherstellt. Die Preisangabe geht ebenfalls gesichert an das Scheckbuch des Kunden zurück und an die Applikation, über die der Kunde die Anfrage abgewickelt hat. Die Applikation des Scheckbuchs läßt sich in einem Mosaic- oder Netscape-Browser integrieren. Im Rahmen einer digitalisierten Unterschrift wird die Transaktion bestätigt und der Scheck ausgefüllt. Der Verkäufer erhält somit keine sicherheitskritischen Informationen. Ein Vorteil des Systems liegt in der flexiblen Preisgestaltung. Die folgende Abbildung illustriert die Ablaufschritte einer Geschäftstransaktion bei Netbill.

[21] http://www.ini.cmu.edu/NETBILL/home.html

Netscape: Flow of Information

File Edit View Go Bookmarks Options Directory Window Help

Location: http://www.netbill.com/merchants/roadmap.html

Merchant Info

NetBill Central
About NetBill
Consumer Services
Shopping
Merchant Info
Index
Help
Send Feedback
Search

Becoming a Merchant | Merchant Software | Configuration | URLs | Architecture

Flow of Information

The 8 steps of a NetBill purchase are:

1. The consumer requests a price quote (by clicking on the URL in the browser)
2. The merchant (price requester) responds with a price quote
3. The consumer accepts the price
4. The merchant (goods assembler) delivers the goods in encrypted form
5. The consumer acknowledges receipt of the goods
6. The merchant (till) contacts the NetBill transaction server to record the transaction and transfer funds
7. The NetBill transaction server confirms that funds have been transferred
8. The merchant (till) sends the decryption key to the consumer and the Money Tool displays the goods in the browser

These steps are shown in the following figure. Note that the product server is only involved in steps 1, 3, and 7; this involvement is further illustrated.

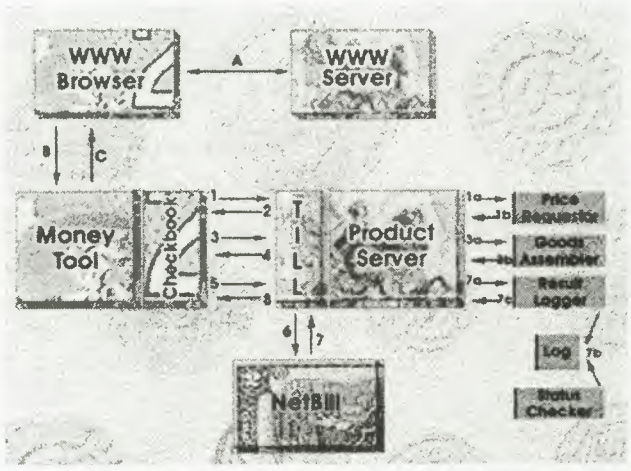

Abbildung 12: Der Weg der Zahlungstransaktion des Netbill-Konzepts

5.2 FSTC Electronic Check Project

Ähnlich dem Netbill-Konzept verfolgt die Bank of Boston zusammen mit dem Financial Services Technology Consortium (FSTC)[22] bestehend aus Banken, Industriefirmen mit Vertretern aus Forschung und Wissenschaft das Ziel des Aufbaus eines elektronischen Scheck-Systems als Zahlungsmittels. Elektronische Schecks werden verrechnet ähnlich dem traditionellen Papiercheck innerhalb der bestehenden finanz- und kreditwirtschaftlichen Infrastruktur [PTS95 S.39]. Der Elektronische Scheck soll von Händlern und Kunden mit seinen Vorteilen genutzt werden wie der traditionelle „Papier"-Scheck. Die Verrechnung erfolgt dabei auf dem bereits bestehenden Abrechnungssystemen der Banken. Das bisherige Scheckbuch wird durch ein elektronisches Scheckbuch, das über Smartcards oder PC-Karten realisierbar ist, ersetzt. Die bisherigen manuelle Unterschriften werden durch digitale Signaturen mittel kryptographischer Techniken realisiert.

In Anlehnung an die bisherige Ablaufphase des Schecks werden aber folgende Vorteile ausgewiesen:

- Überprüfung der Deckung von Schecks;
- Schrittweise Erfassung aller am Prozeß beteiligter Personen über digitale Signaturen;
- Möglichkeit der Integration in weitere elektronische Bestellung- und Zahlungssysteme;
- Registrierung aller ausgegebenen Schecks über eine externe Software (application programme interface API).

[22] http://www.fstc.org/projects/echeck

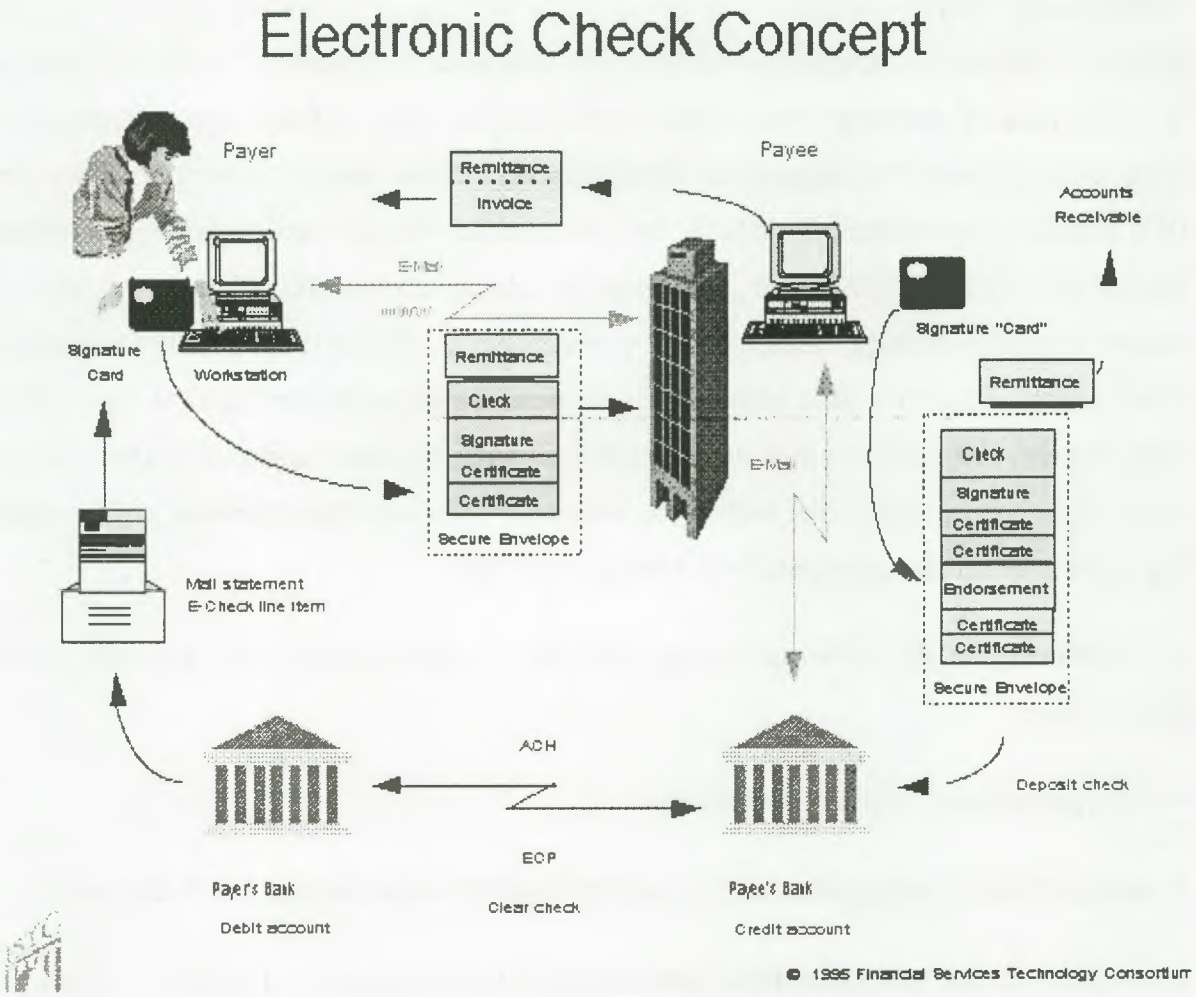

Abbildung 13: Transaktionsablauf nach dem FSTC-Electronic Check-Konzept

Das Projekt befindet sich derzeit noch in der Entwicklung. In der zweiten Hälfte des Jahres 1996 war die Einführung einer Pilotphase geplant [PTS9540].

6. Konzepte basierend auf Kreditkarten

6.1 First Virtual (ohne Kryptographie)

Die Firma First Virtual[23] gilt als Pionier bei Systemen mit Email-Rückfrage, bei denen auch ohne kryptographische Verfahren ein sicherer Zahlungsverkehr ermöglicht wird. Um eine Information oder Ware zu kaufen, wendet sich der Käufer via Email oder SMXP (Simple Mime Exchange Protocol) an First Virtual und gibt dabei seine PIN (Persönliche Identifikationsnummer) bei First Virtual an. First Virtual sucht dann in seiner Datenbank die PIN des Kunden und die damit registrierte Email-Adresse. An diese Email-Adresse wird eine Nachricht geschickt, mit der Bitte um Bestätigung der Transaktion.

Die PIN-Nummer des Käufers wird einmalig eingerichtet, dabei werden via Telefonanruf die sensitiven Kreditkarteninformationen übertragen, so daß bei späteren Transaktionen diese Daten nicht über das Internet geschickt werden müssen. Der Anbieter gibt First Virtual einmalig seine Bankverbindung via normaler Post an. Weil die PIN nur bei First Virtual Bedeutung besitzt und jeweils eine Bestätigung per Email erfolgen muß, ist Betrug nur durch einen Einbruch in den Account des Käufers möglich, da erst dann dessen Email abgefangen werden kann. Für jede Transaktion werden vom Anbieter ein Prozentsatz des Verkaufswerts als Provision für First Virtual abgezogen. Die Registrierung des Kunden kostet 2 US-Dollar und die des Anbieters 10 US-Dollar. Der eigentliche Zahlungsakt ist anonym, da sowohl Käufer wie Verkäufer Mail-Pseudonyme verwenden können. Der Vorteil dieses Systems liegt in dem einfachen und sicheren Verfahren der Zahlungsabrechnung[24].

---

[23] http://www.fv.com

[24] Einen ähnlichen Ansatz verfolgen das „Internet Shopping Network“ und „Compuserve“.

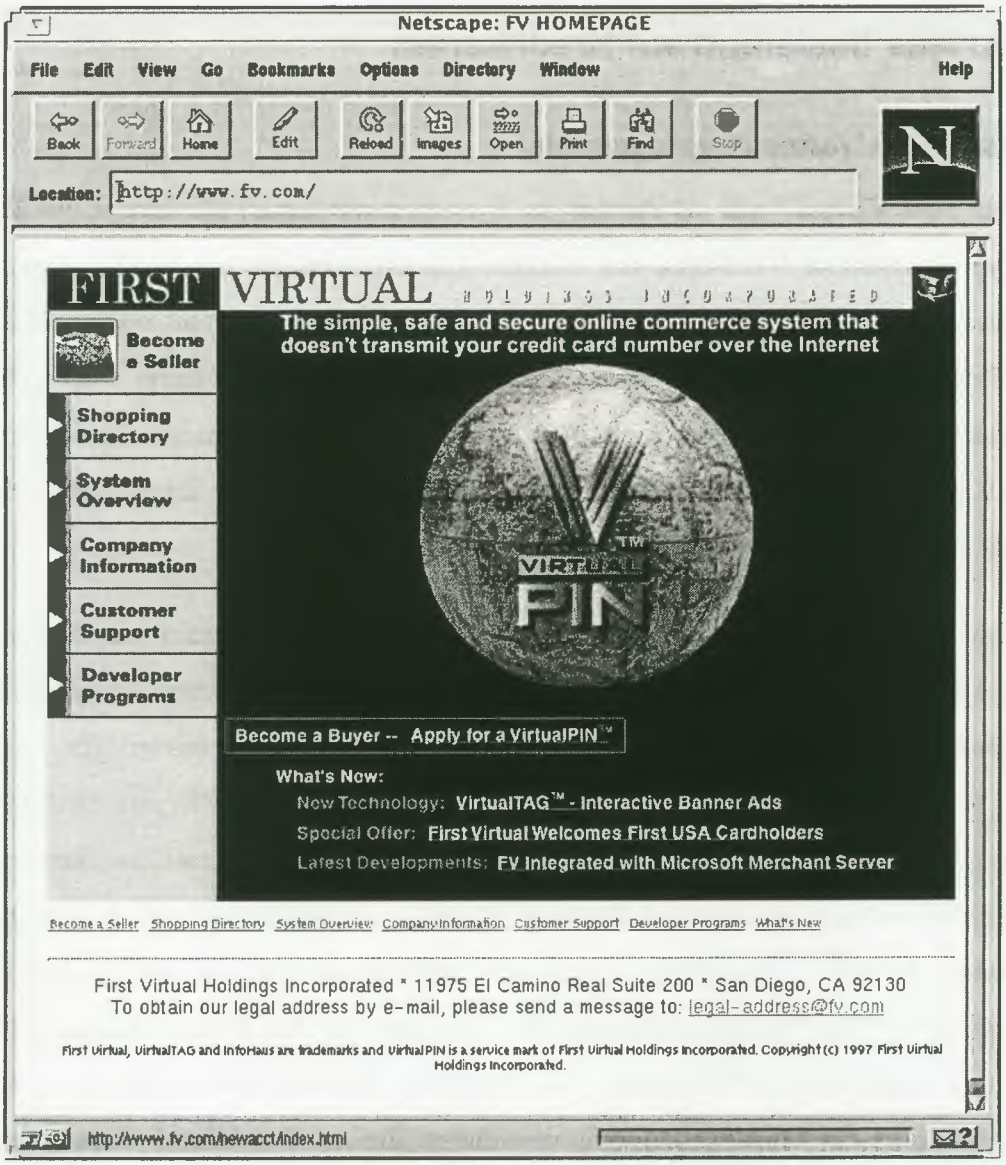

Abbildung 14: First Virtual Hompage

6.2 Netscape Commerce Server

Nicht anonymisierte Zahlungssysteme basieren auf Kreditkarten sind, verglichen mit dem vorher beschriebenen anonymen Zahlungssystem am Beispiel von First Virtual, am weitesten verbreitet. Zu den bekanntesten zählen Referenzimplementationen basierend auf der Erweiterung des HTTP-Protokolls mit SSL (Secure Socket Layer) der Firma Netscape und das S-HTTP-Protokoll der Firma Terisa Technologies, eine Entwicklungsgesellschaft gegründet von Enterprise Integration Technologies (EIT) und RSA Data Security. Terisa entwickelte auch den SSL-Standard, den sie an die Firma Netscape (mit Exportrestriktionen versehen) weiterverkaufte. Das primäre Geschäft von Netscape gründet sich auf die kommerziell

ausgerichtete „Commerce-Server"-Software. Die weltweitbekannte Browsersoftware wird bis auf Firmenlizenzen praktisch verschenkt. Mit der Commerce-Server-Software enthält der Kunde eine „high-performance" Software, die einen sicheren elektronischen Handel über das Internet und andere TCP/IP Netzwerke mit dem SSL-Protokoll ermöglicht. Netscape's Commerce Server-Software wurde entwickelt für Online-Transaktionen und dient dem elektronischen Datenaustausch von sensitiven Daten (z. B. Kreditkarteninformationen bei Bestellungen, etc.). Sie wird im größeren Umfang von Shopping Malls und im Online Banking genutzt. Online-Dienste wie Compuserve und AOL setzen wiederum auf den Standard S-HTTP von Terisa, während Zeitungsverlage und Hosts z. B. Knight Ridder und IDG sich bei SSL engagierten. Den Bekundungen beide Standards SSL und S-HTTP zu integrieren und zu einem gemeinsamen Standard zu erheben ist bis heute noch nicht realisiert worden.

7. Framework für Zahlungssysteme

7.1 Java Electronic Commerce Framework (JECF)

Die bei SUN Microsystems[25] für die Internet-Programmiersprache Java[26] zuständige Business Unit JavaSoft hat Anfang Dezember 96 zwei Neuheiten angekündigt, die im ersten Quartal 1997 verfügbar sind. Neben einem Java Development Toolkits (JDK1.1) wurde ein Java Electronic Commerce Toolkit basierend auf dem Java-Electronic Commerce Framework (JECF) entwickelt. JECF beinhaltet eine Reihe von Tools und Utilities, die zukünftige Electronic Commerce Softwareentwicklungen durch den Einsatz Java basierter Applikationen erleichtern soll. JECF versteht sich dabei als ausbaufähiges Electronic Commerce Framework für die Entwicklung business orientierter Applikationen für das Internet. Das Paket wird im 1.Quartal 1997 an registrierte Entwickler lizensiert [Com96 S.13].

JECF stellt eine breite Palette von Zahlungsmethoden zur Verfügung, die über sogenannte Java Applets und Cassettes implementiert werden. JECF beinhaltet fünf vorgefertigte Typen für bekannte Zahlungsverfahren, wie z. B. Kreditkartentransaktionen nach dem SET-Protokollstandard, SmartCards nach dem Mondex-Verfahren, Electronic Check und eine von CyberCash (siehe Kap. 9.1) entwickelte elektronische Geldbörse für Kleinstbeträge (Java-Wallet).

Die Komponenten des JECF basieren auf der objektorientierten Programmiersprache Java, mit der von einem Web-Server abgelegte plattformunabhängige Java-Applets über einen Java fähigen WWW-Browser auf dem PC des Kunden gestartet werden können. Innerhalb des Toolkits befinden sich auch ein programmierter virtueller Einkaufswagen (Java Electronic Shopping Cart), mit dem der Online-Kunde seine Artikel sammeln und zum Schluß zentral abrechnen kann. Dies geschieht zunächst über den PAY-Button, der den JECF-Zahlungsprozess aktiviert. Nachdem die Identität über ein Paßwort überprüft wird übernimmt ein Softwaremodul (Payment Cassette), das auf dem PC des Kunden gespeichert wird, die Datenübertragung. Dem Kunden stehen für den Kaufprozeß 3 Applets zur Verfügung (identity applet, tally applet und payment instrument selection applet). Das erste Applet stellt

---

[25] http://www.sun.com

[26] http://www.java.sun.com

Informationen über den Verkäufer bereit, das zweite zeigt Informationen über die gekauften Waren und den Preis an und mit Hilfe des dritten Applets kann der Kunde seine bevorzugte Zahlungsvariante auswählen. Nach dem Bestätigen der Applets werden die Daten von der Payment Cassette zum Server übertragen und mit dem Status noch in Schwebe befindlicher Transaktionen des Kunden abgelegt. Der Prozeß kann mehrere Sekunden bis Minuten andauern. Ist der Zahlungsprozeß abgeschlossen, werden die schwebenden Transaktionen in „getätigte" überführt und gespeichert. Im Falle von Systemabstürzen bzw. Netzwerkabbrüchen können diese Daten genutzt werden, um die Transaktion zurückzusetzen.

Der Vorteil dieses Systems liegt in der Offenheit und möglichen Adaptierbarkeit auf viele existierende Zahlungssysteme und ihrer Kombinationen, die über Java-Applets realisiert werden können. Eine kleine Einschränkung liegt in der Mindestkonfiguration eines Java fähigen Browsers, der eine 32-Bit Betriebssystemkonfiguration (Windows95, Unix etc.) erforderlich macht [ABI96 S.44].

7.2 IBM`s Internet Keyed Payment Protocol (iKP)

Die „Security Groups of IBM Research[27]" in Hawthorne und Zürich[28] haben verschiedene Sicherheitsprotokolle für elektronische Zahlungen, sogenannte Internet Keyed Payment Protocols iKP entwickelt, die als offener Standard mit jedem Browser und Server plattformunabhängig betrieben werden kann. Neben dem Prototyp auf Basis von Kreditkarten, sind auch Zahlungsvarianten z. B. elektronische Schecks und Debitkarten für Lastschriftverfahren in Vorbereitung. Der erste Prototyp ist als reine Softwarelösung konzipiert, wobei von IBM auch an hardwareunterstützende Lösungen gearbeitet wird. Die iKP-Technologie basiert auf der bekannten RSA public-key Kryptographie und verwendet je nach Anforderungen einen oder bis zu drei öffentliche Schlüssel im Rahmen unterschiedlicher Protokolle (1KP bis 3KP). Das Zahlungssytem setzt dabei 3 Parteien voraus, bestehend aus Kunde, Händler und einem Gateway. Der Gateway übernimmt dabei die Verbindung zum jeweiligen Zahlungsinstitut. In Abhängigkeit der Anforderung können die Protokolle 1-3 stufenweise eingeführt werden .

---

[27] http://www.ibm.com

[28] http://www.zurich.com/Technology/Security/extern/ecommerce/ikp_reference.html

1KP Variante:

Bei diesem Protokoll besitzt der Gateway ein Schlüsselpaar, während Händler und Kunde nur über den öffentlichen Schlüssel des Gateways verfügen. Die Authentifizierung des Kunden erfolgt über die Kreditkartennummer, die verschlüsselt mit der PIN übertragen wird.

2KP Variante:

In diesem Protokoll besitzt auch der Händler Schlüsselpaare (public und private keys), so daß der Kunde die Identität des Händler überprüfen kann, ohne die Notwendigkeit einer dritten Instanz. Der Kunde wird über die Kreditkartennummer und der PIN, wie im ersten Protokoll (1KP) authentifiziert.

3KP Variante:

Dieses Protokoll gilt als das Aufwendigste, aber auch sicherste Zahlungsprotokoll innerhalb der iKP-Familie. Neben dem Gateway und dem Händler besitzt auch der Kunde ein Schlüsselpaar. Der Nachweis der Authentizität des Kunden wird nicht nur über die Kreditkarte und der PIN gewährleistet, sondern wird darüber hinaus über digitale Unterschriften erzeugt. Notwendig für diese Variante ist aber eine aufwendige Infrastruktur für die Zertifikaterstellung, um die öffentlichen Schlüssel der Kunden zu zertifizieren.

Der Einsatz von iKP setzt eine Zertifizierungsinstanz voraus, die einen geheimen, privaten und öffentlichen Schlüssel besitzt, der für alle Kunden zugänglich ist. Da die iKP-Familie keine Verschlüsselung der zu übertragenden Informationen unterstützt, ist es sinnvoll die IBM Protokolle zusammmen mit der S-HTTP-, SSL- oder SET-Technologie zu kombinieren und zu implementieren.

7.3 Semper (Secure Electronic Marketplace for Europe)

SEMPER[29] ist ein Forschungsprojekt, das von der Europäischen Kommission im Rahmen des Advanced Communications Technologies and Services (ACTS) Programms (AC026) gefördert wird und sich mit der Entwicklung eines sicheren elektronischen Marktes befaßt. SEMPER wurde im September 1995 von einem interdisziplinären Konsortium bestehend aus

[29] http://www.semper.org

18 Projektpartnern gestartet und ist befristet für die Dauer von 3 Jahre. Die Zusammensetzung der Partner aus den Bereichen Telekommunikation, Informationstechnik, Finanzsystemen, Handel und Wissenschaft ergeben ein vertikal integriertes Projekt aus allen den elektronischen Handel unterstützenden Parteien. Zu den Teilnehmer gehören u.a. der Otto-Versandhandel, FOGRA und EUROCOM. Aus wissenschaftlicher Sicht ist unter anderem die Universität St. Gallen (IWI) an dem Projekt beteiligt.

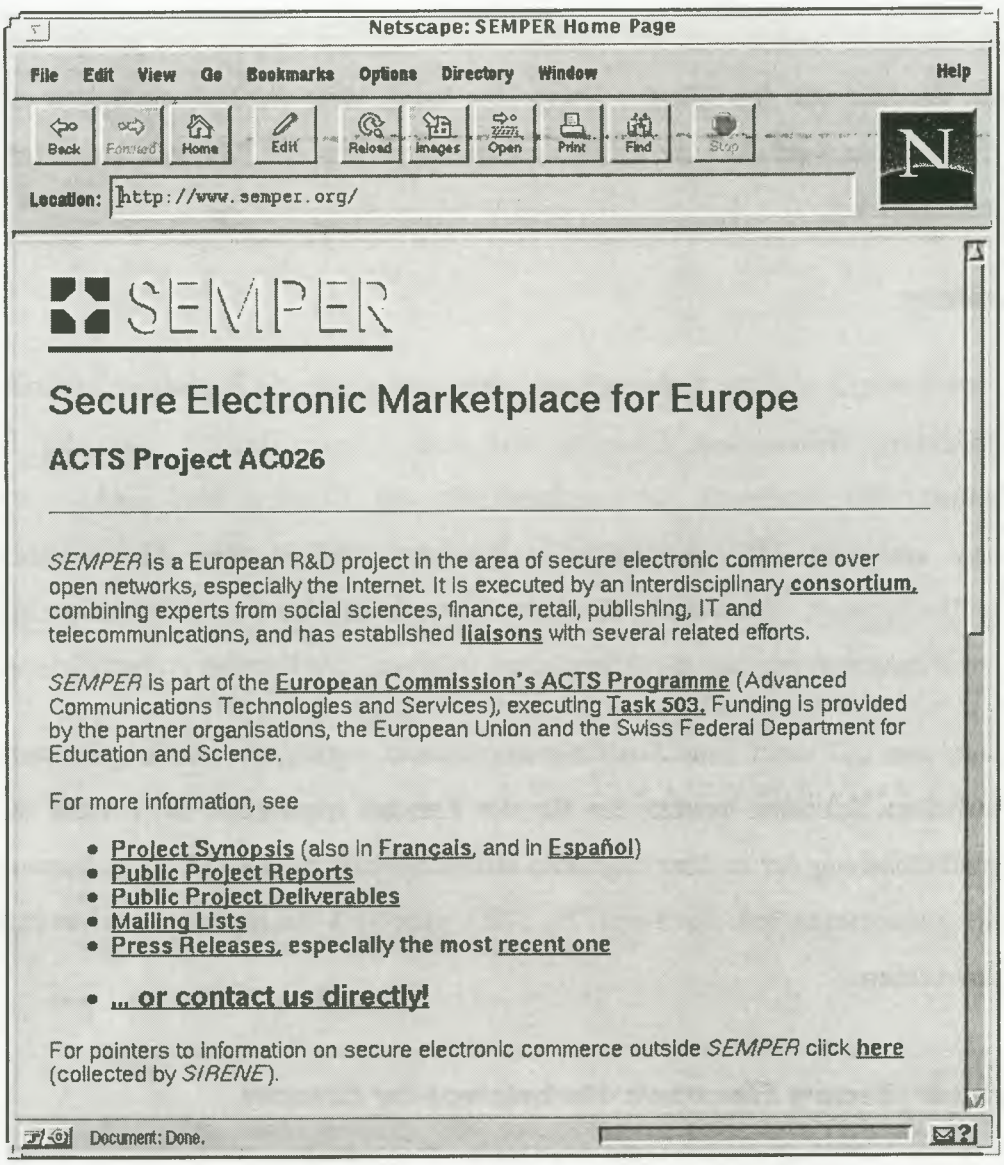

Abbildung 15: Informationsseite zu SEMPER

Im Gegensatz zu einigen existierenden Diensten und Projekten, die auf geschlossene Lösungen zielen und auf elektronische Zahlungen fokussieren, zielt SEMPER auf eine offene Architektur für die Integration der verschiedenen Protokolle und Komponenten zu einem sicheren elektronischen Marktplatz, der ein einfaches Teilnehmen für Anbieter und Käufer

bietet. Der Ansatz existierende Komponenten rund um das WWW zu einem vollständigen System für elektronische Märkte zu integrieren, und die Ergebnisse möglichst schnell in realen Versuchen auf dem Internet zu testen, verspricht eine baldige Lösung der technischen Fragen zum elektronischen Markt. Dabei werden außer den technischen auch nicht technische Fragen und Anforderungen untersucht. So wird zum Beispiel die Frage der Rechtsverbindlickeit elektronischer Transaktionen untersucht oder die Akzeptanz der verschiedenen Protokolle bei den Benutzern. Insgesamt verfolgt SEMPER die folgende Zielsetzung:

- Detaillierte Beschreibung der legalen, kommerziellen, sozialen und technischen Anforderungen und Optionen für einen elektronischen Markt;
- Entwicklung eines vollständiges Modells für eine offene Architektur eines sicheren elektronischen Marktes, unabhängig von spezifischer Hardware, Software und Netzwerkarchitektur;
- Darstellung von Spezifikationen, Design- und Prototyp-Implementierungen von Diensten, die den elektronischen Markt in Bezug auf Electronic Commerce (offering, ordering, payment, delivery etc.) ermöglichen und Evaluierung der Ergebnisse von Tests in Pilotversuchen;
- Entwicklung von notariellen Diensten, die einen „fairen Austausch" von Waren und Dienstleistungen ermöglichen (Vertragsunterschriften, Kaufverträge, etc.);
- Multimediale spezifische Sicherheitsdienstleistungen (z. B. intellectual property rights);
- Bereitstellung und Verbreitung von Informationen aus Wissenschaft und Technik, zu Standardisierungen und Entwicklungen im Bereich Electronic Commerce, unter Berücksichtigung der Ergebnisse anderer ACTS Projekte der Europäischen Kommission.

Aufgrund der oben skizzierten Zielsetzung geht SEMPER von der Dominanz des WWW's und seiner zukünftig immer stärker werdenden Nutzung für den elektronischen Markt aus, wie z. B. Online Verkauf, Bestellung, Bezahlung, Publizieren und Austausch von Geschäftsdokumenten. Die erste Version des elektronischen Marktplatzes basiert auf dem WWW hat die Untersuchung verschiedener Protokolle zur Unterstützung des elektronischen Zahlungsverkehrs zum Gegenstand. SEMPER benutzt und integriert bestehende

Architekturen, Tools und Dienste, die sich am Markt etabliert haben. Sicherheitstoolkits entwickelt von Cryptomathic und der GMD unterstützen die notwendige Authentifizierung und Zertifizierung. Systeme von DigiCash (Ecash) und IBM (iKP/SET) für Kreditkarten unterstützen den Zahlungsverkehr. Die Entwicklung des Semper Projektes berücksichtigt sich abzeichnende Marktanforderungen und „state of the art" Entwicklungen in Fragen von Security, Online-Informationsdiensten und Mehrparteien-Sicherheitsanforderungen (multi-party security). Der Schutz der Privatssphäre wird abschließend im Konzept des Semperprojektes eine besondere Bedeutung beigemessen.

7.4 Brokat`s X.Presso Security Package

Die deutsche Softwarefirma Brokat[30] aus Böblingen entwickelte als erstes Unternehmen eine auf der Java-Technologie und kryptographische Algorithmen basierende Sicherheitssoftware, namens X.Presso Security Package 1.0, die auch außerhalb der USA eine sichere, nicht brechbare 128 Bit-Chiffrierung von vertraulichen Online-Transaktionen im Internet gewährleistet. Damit existiert erstmals die Möglichkeit, Kryptographie-Beschränkungen in Internet-Browsern außerhalb der USA zu umgehen, ohne zusätzliche Software- oder Hardware-Installationen auf den Rechnern der Internet-Kunden. Das bisherige Sicherheitsdefizit bezüglich der geringen Schlüssellänge von 40 bzw. 56 bit aufgrund der US-Exportrestriktionen, hinderte insbesondere Finanzdienstleister und Handelshäuser in Europa daran, transaktionsgesicherte Dienstleistungen wie Electronic Banking oder Online-Shopping im Internet zu etablieren. Brokat kooperiert mit Siemens Nixdorf, IBM und Netscape und entwickelt Softwarelösungen für Bankhäuser (Deutsche Bank, Bank24, Direkt Anlage Bank, Advance Bank). Für das X.Presso Security Package erfolgt gegenwärtig eine unabhängige Sicherheitsprüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) basierend auf den europäischen Sicherheitskriterien (ITSEC).

[30] http://www.brokat.de

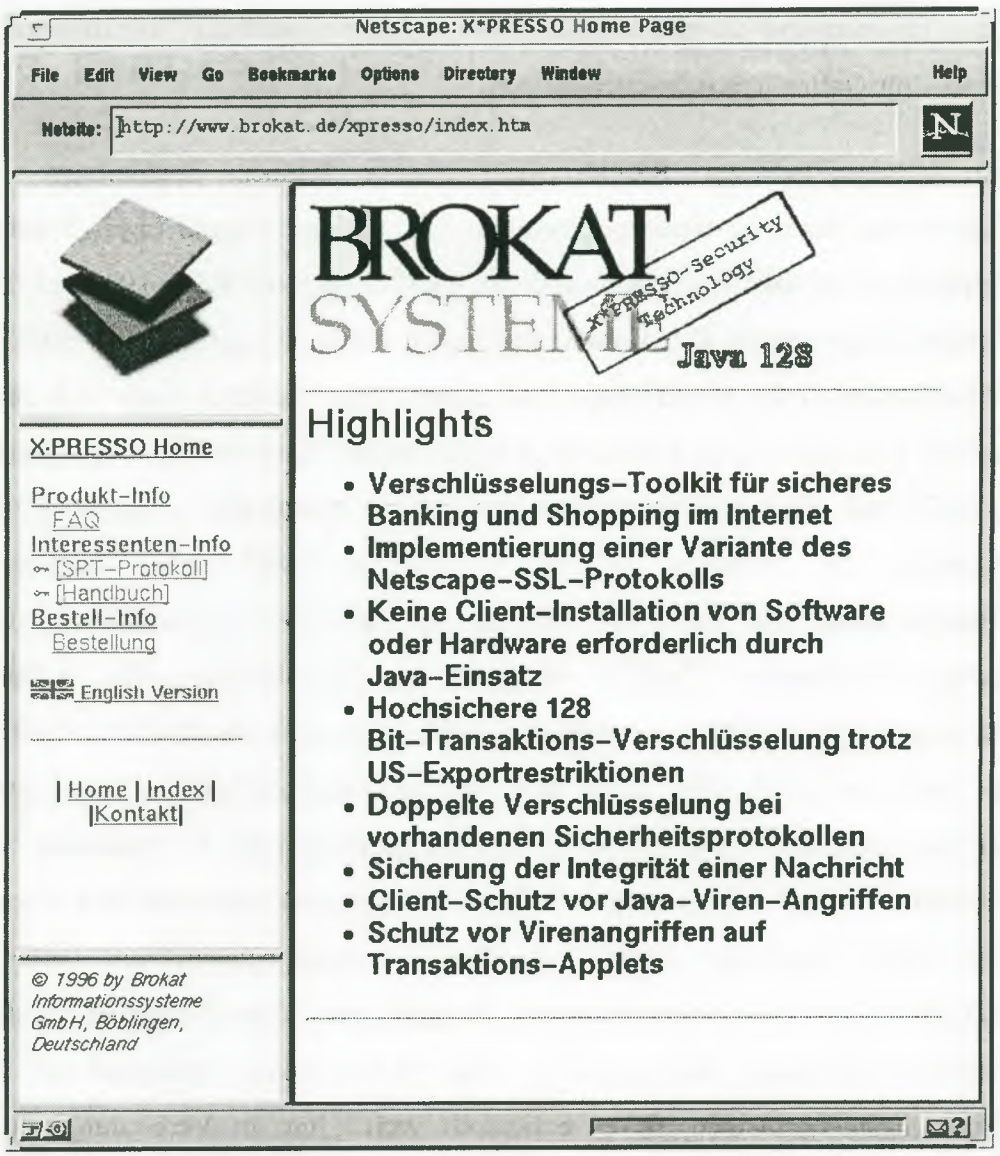

Abbildung 16: Informationsseite von Brokat zu X.Presso Security Package

Das X.Presso Security Package besteht aus einem Security Server, der im bestehenden Systemumfeld des Internets-Anbieters integriert wird, und aus den konfigurierbaren Java-Verschlüsselungsklassen X.Presso Java Security Classes, mit denen beliebige kundenspezifische Java-Transaktions-Applets gestaltet werden können. Diese Applets können von jedem Java fähigen Sicherheits-Browser, z. B. Netscape Navigator oder Microsoft Internet Explorer, geladen und kundenspezifisch angepaßt werden. Über sogenannte Integrity Check Plugins werden die geladenen Java-Applets und die Java-Runtime in dem Browser vor mögliche Virus-Attacken überprüft, bevor eine Transaktion über das Internet freigegeben wird. Um auch die Plugins vor Übergriffen zu schützen steht als Schutz ein kontinuierlicher täglicher Upload-Service von Plugins für den Kunden bereit. Diese Plugin-Technologie

erlaubt dem Internetnutzer kleine zusätzliche Programme zu installieren, die die Funktionalität des Browsers für Online-Transaktionen steigert.

Mit dem X.Presso-basierten SRT-Protokoll (Secure Request Technology) wurde in Anlehnung an das bekannte Netscape Protokoll SSL (Secure Socket Layer Protokoll) eine leistungsoptimierte Protokollspezifikation durch die Nutzung von RSA-1024 und IDEA-128 Bit Algorithmen entwickelt. Die Verschlüsselungs-Kommunikation über das SRT-Protokoll wird auf der Request- oder Anwendungsebene durchgeführt. Dadurch ergibt sich der Vorteil, daß eine SRT-Verschlüsselung zusätzlich zu existierenden Browser-Verschlüsselungen z. B. SSL, S-HTTP bzw. PCT genutzt werden, um darüber hinaus eine zusätzliche (doppelte) Verschlüsselung zu erzeugen [PTS96 S.37]. So wird eine weitaus höhere Transaktionssicherheit (40 plus 128 Bit) erzeugt, als die vergleichbar in den USA zugelassenen Web-Browser. Zunächst unterteilt das SRT-Protokoll die zu übertragene Nachricht in gleich große Blöcke, berechnet einen Hashwert und verschickt die Nachricht. Die Integrität einer Nachricht wird durch den Message Authentification Code (MAC) als Hashwert oder digitaler Fingerabdruck erzeugt, der zusammen mit der Nachricht verschickt wird. Das SRT Protokoll 1.0 unterstützt die MAC Algorithmen MD5 und SHA (Secure Hash Algorithm). Beim Empfänger werden die Blöcke getrennt dechiffriert, vom Message Authentification Code (MAC) oder Hashwert überprüft, die Blöcke zusammengeführt und an die eigentliche Anwendung weitergegeben. Das SRT-Protokoll unterstützt nur begrenzte Autentifizierungsmechanismen, da es entwickelt wurde, um in Verbindung mit anderen Verschlüsselungsprotokolle integriert zu werden, die diese Sicherheitsaspekte berücksichtigen. Das Brokat Security Package beinhaltet schlüsselfertige Transaktionslösungen, die speziell für Finanzdienstleister und Geldinstitute entwickelt wurde.

7.5 Netscape Livepayment

Als Erweiterung zu der bereits bestehenden Commerce Server-Software entwickelte die Firma Netscape ein Erweiterungspaket namens „Netscape Livepayment“, als Entwicklungsumgebung für den Aufbau einer WWW-basierenden Electronic Commerce Applikation. Netscape`s Livepayment nutzt die bereits eingeführte SSL-Technologie der Kreditkartenverschlüsselung in Anlehnung an SET und stellt mit dem Produkt „Livepayment“ ein Frameworkt zur Verfügung, das es Händlern erlaubt kommerzielle und kostengünstige Websites zu erstellen.

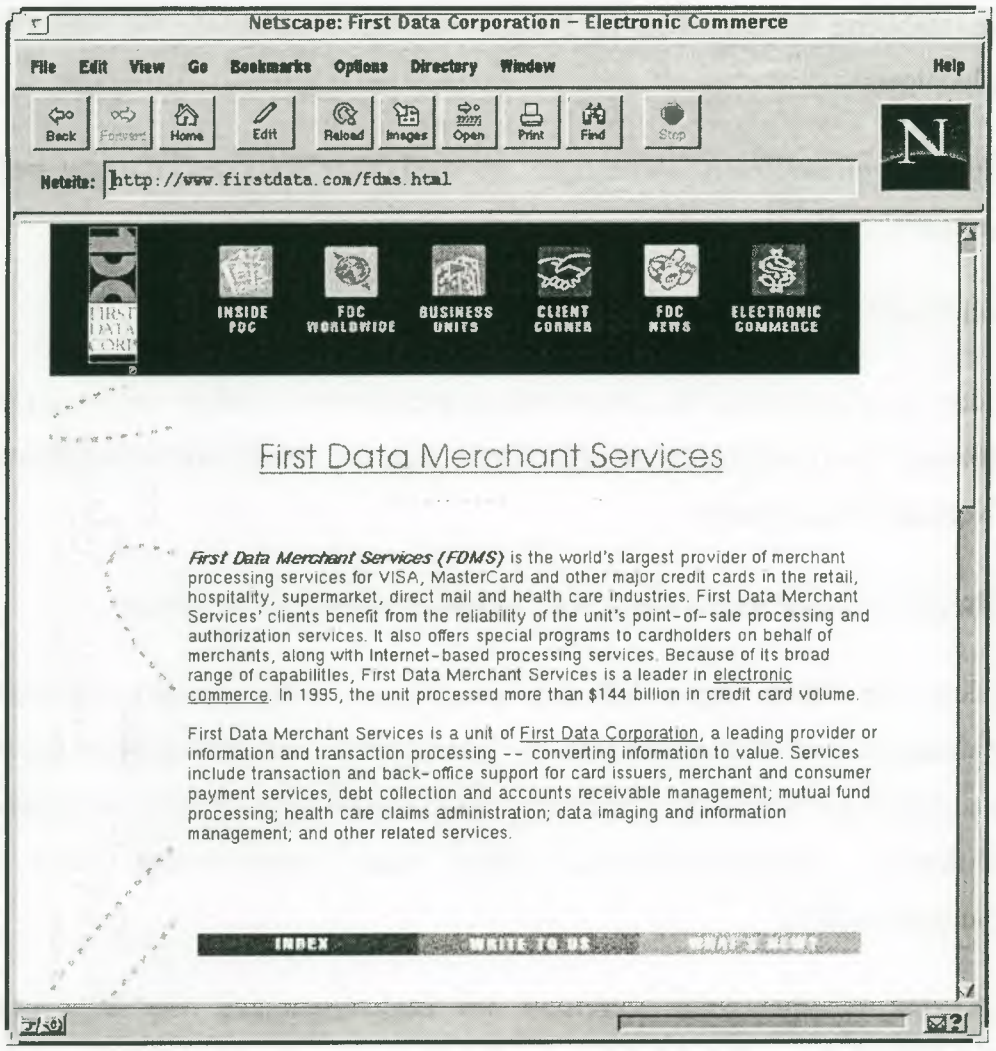

Abbildung 17: Kooperation von Netscape und First Data Merchant Service (FDMS)

Livepayment besteht aus den Produkten „paymentprozessor“, einem Satz von LiveWire „commands“, „objectives“, „utility-commands“ und einem „administrative interface“. LiveWire beinhaltet HTML-Texteditoren, Funktionen für Datenbankinterface und unterstützt Java-Script. Im Gegensatz zu einer „Verschlüsselung“, die bereits mit dem Protokoll SSL eintwickelt wurde, liegt der Vorteil in der Integration der Protokollspezifikation mit Kreditkartenautorisierungsstellen und Banken. Das Ziel ist es, den sicheren Zahlungsprozeß mit „Leben“ zu erfüllen, deshalb auch die Vermutung der Namensgebung: „Livepayment“. Die Vorteile nach Angaben des Herstellers sind:

1. niedrige Kosten und geringe Entwicklungszeiten bei der Implementierung einer kommerziellen Online-Applikation;

2. bereits etablierte Schnittstellen zu Finanz- und Kreditinstituten, die eine Realisierung beschleunigen;

3. die Nutzung von hardwareunabhängigen „standard client interfaces", die eine große Anzahl von potentiellen Kunden und unterschiedlichen Browsern ansprechen.

Der Geschäftsprozeß von Livepayment gestaltet sich wie folgt:

- Nachdem der Kunde seine Kaufentscheidung getroffen hat, wird er von der Livepayment-Applikation des Händlers aufgefordert Name, Adresse, Kreditkarteninformationen mittels SSL verschlüsselt zu senden;

- Die Bestell- und Zahlungsinformationen werden verschlüsselt übertragen;

- Nachdem die Daten beim Händler eingegangen sind, werden sie durch einen verschlüsselten Kreditkartenschein an die Kreditkartenautorisierungsstellen weitergeleitet. Dies geschieht mit Hilfe eines CardProzessors innerhalb der Livepayment-Applikation. Der verschlüsselte Kreditkartenschein dient der Autorisierung und späteren Zahlungstransaktion;

- Die Kreditkartenorganisation autorisiert den Zahlungsvorgang oder lehnt eine weitere Bearbeitung ab;

- Im Falle der positiven Autorisierung, wird im nächsten Schritt der Zahlungsvorgang erfaßt und die Kreditkartenbuchung vorgenommen, die im Stornierungsfall vom Händler zur Gegenbuchung auch wieder verwendet wird;

- Der Zahlungsausgleich zwischen der Bank des Händlers und der Kreditkartenorganisation verläuft wie bekannt. Die Kreditkartenorganisation überweist das Geld vom Kundenkonto auf das Konto des Händlers.

Das Konzept von Livepayment zeigt einen Weg der Etablierung eines sicheren Zahlungsprozesses unter Einbeziehung der Kreditkartenorganisation und des Bankenbereichs an. Da Livepayment vorläufig nur auf Kreditkartentransaktionen beschränkt ist, wird das große Potential der Kundschaft mit ihren Zahlungsgewohnheiten und -wünschen noch nicht erfaßt. Eine Einführung ist auch problematisch, da zwischen Händler, Kreditkartenorganisation und Banken strategische Allianzen aufgebaut werden müssen. Zum

jetzigen Zeitpunkt verweist Netscape auf einige Kooperationen mit Banken und Finanz- und Kreditorganisationen in den USA hin, die mit dem Konzept zusammenarbeiten. In Europa bzw. in Deutschland wird es aber noch einige Zeit dauern, bis ähnliche Kooperationen gebildet werden.

8. Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) bezeichnet den elektronischen Austausch strukturierter Daten (Dokumente) über Geschäftstransaktionen, z. B. Bestellungen, Buchungen, Abrechnungen mittels zwischenbetrieblich oder branchenindividuell vereinbarter Formate zwischen Computer-Applikationen. Im Gegensatz zu anderen, unstrukturierten Verfahren des elektronischen Datenaustausches, z. B. electronic-mail[31], ermöglicht EDI eine direkte Übernahme der übermittelten Daten in entsprechende Anwendungsapplikationen der beteiligten Geschäftspartner, woraus auch eine teilweise vollmaschinelle Verarbeitung der angefallenen Daten resultiert. Für die automatische Interpretation durch Rechner sind die Nachrichten exakt zu definieren, vorhergehend muß eine entsprechende Software installiert werden. EDI setzt formalisierte Datenstrukturen voraus und ist damit auf eine begrenzte Zahl gut definierbarer Nachrichtentypen (z. B. Bestellung, Rechnung, Lieferavis) beschränkt. Es wird nur in geschlossenen Benutzergruppen verwendet, die sich auf die Nachrichtendefinitionen einigen.

Ziel von EDI ist die Ablösung der heute vorherrschenden, papiergebundenen Geschäftsabläufe durch deren Abwicklung mittels elektronischer Dokumente und Übertragung. Dies bietet den Vorteil schnellerer Übermittlung, automatisierbarer Abläufe, sowie Arbeits- und Kostenreduktion durch den Wegfall von Datenerfassung und der Reduzierung von Erfassungsfehlern. Obwohl EDI-Konzepte seit mehr als 15 Jahren in Europa und Nordamerika existieren, ist ihre Marktdurchdringung und Akzeptanz in weiten Teile der Industrie und des Handels noch unterentwickelt [ABI94 S.49].

Die Zielgruppe für die Anwendung von EDI waren bisher der nicht private Nutzer, allen voran Industrie- und Handelsunternehmen sowie der Banken- und Versicherungsbereich, denen der Einsatz von EDI mit den Vorzügen der effizienten Kommunikationsstruktur zwischen den Handelspartnern und der schnellen Übertragung der Informationen Kostenvorteile im Wettbewerb versprach. Die bisherige Ausrichtung von Standards vorwiegend für den

---

[31] Bei elektronischen Übertragungssystemen werden zwischen Personen und/oder Rechnern Nachrichten ausgetauscht, die durch Dateien beliebigen Inhalts ergänzt werden können. Entscheidendes Merkmal im Gegensatz zu EDI ist aber, daß die Nachrichteninhalte durch die Empfangsperson interpretiert werden müssen.

kommerziellen Bereich ist aber kein Argument gegen die Integration des privaten Kunden in den EDI-Kreislaufs.

Im folgenden soll auf verschiedene Nachrichtenstandards und besonders auf den in Europa weit verbreiteten Standard UN/EDIFACT "United Nations/Electronic Data Interchange for Administration, Commerce and Transport" verwiesen werden, der auch im elektronischen Zahlungsverkehr zum Einsatz kommt. Unglücklicherweise existiert kein einziger universeller Standard, der die verschiedenen Typen von geschäftlichen Transaktionsformen zuläßt. EDIFACT ist ein offizieller internationaler Standard neben anderen EDI-Formaten, z. B. International Air Transport Association (IATA), Organisation for Data Exchange Through Tele-Transmission (ODETTE), Trade Data Interchange (TDI), American National Standard (ANSI X.12), Society of Worldwide Interbank Financial Telecommunication (SWIFT). Einige dieser Standards haben den Nachteil entweder nur für einzelne Länder oder Branchen oder auf beides beschränkt zu sein [Mau95].

8.1 EDI und Internet

Es ist unbestritten, daß Unternehmen durch den Einsatz von EDI nicht nur die Übertragung von Geschäftsdaten und damit ihre Leistungs- und Logistikprozesse beschleunigen, sondern auch neue Geschäftsfelder eröffnen und ihre organisatorischen Strukturen auf die Geschäftsprozesse ausrichten können.[32]Ungeachtet der technischen Fortschritte bei Netzen, Diensten und Austauschformaten konnte EDI jedoch in vielen Fällen nur dort realisiert werden, wo starke Unternehmen bzw. Branchen ihre Geschäftspartner "überzeugten" (No EDI - No Buy). EDI existiert seit mehr als 15 Jahren in Nordamerika und Europa. EDI-Nachrichten wurden bisher über sogenannte value-added networks (VAN's) basierend auf Telefonleitungen entsprechender Anbieter (Mailboxes provided by Third Parties) verschickt. Dies ist insbesondere bei weltweiten Handelsbeziehungen günstiger als proprietäre Netzwerke.

Das Internet mit seinem weltumspannenden Kommunikationsnetz verspricht neben seinen Einsatzmöglichkeiten als Informationsquelle und Medium für Marketing und Vertrieb aufgrund der offenen Informations- und Kommunikationsstruktur auch die kommerzielle

[32] Ansatzpunkte für die Verbindung von EDI und Internet zeigen Klein und Lindemann (IWI St. Gallen) in ihrem Artikel „Die Nutzung von Internet-Diensten im Rahmen des elektronischen Datenaustausches - Architekturvarianten und ein Anwendungsszenario (http://www-iwi.unisg.ch/cc/em/papers/nutzung.html) auf.

Nutzung z. B. im Rahmen von EDI-via-Internet-Anwendungen [Pey96]. Das gute Preis/Leistungsverhältnis im Gegensatz zu VAN's, die einfache Handhabung, starke Zuwachsraten, und die Möglichkeiten der direkten, unproblematischen Anbindung unterschiedlicher Netze sprechen für den kommerziellen Einsatz von EDI über das Internet[33]. Insbesondere die offene Infrastruktur des Internets gewährleistet direkte Kommunikationsverbindungen zum potentiellen Geschäftspartner oder privaten Nutzer und ergänzt die Defizite von EDI, die bisher an einer globalen EDI-Anwendung und Ausbreitung ursächlich verantwortlich waren, da effiziente EDI-Anwendungen häufig an einer unzureichenden Infrastruktur für die Übertragung von EDI-Nachrichten scheiterte. Insofern besitzen Internet und EDI komplementäre Potentiale. Voraussetzung hierfür ist aber die problemlose Übertragung von EDI-Nachrichten auf dem Internet. Möglich wird sie durch eine Art Briefumschlag, den sog. MIME (Multipurpose Internet Mail Extension), der Manipulationen und Verfälschungen von Inhalt und Absender erschweren soll. Dieses Protokoll integriert EDI, Text-, Graphik etc. in Electronic Mail und erlaubt damit die Übertragung von EDI-Daten unabhängig von den jeweils zugrunde liegenden EDI-Standards [MU95].

Im weiteren steht aber speziell die Thematik des Bestell- und Zahlungsverkehrs mittels EDI im Mittelpunkt der Betrachtung. Derzeit wird mittels EDI vornehmlich der Austausch standardisierter, die Geschäftsabwicklung begleitende kommerzielle Dokumente, wie Rechnungen, Aufträge, Auftragsbestätigungen etc. vorgenommen, um primär den Kaufprozeß zu beschleunigen. Financial Electronic Data Interchange (FEDI) im Sinne von Autorisierung von Zahlungsanweisungen über Kreditinstitute findet sich bisher nur in Einzelfällen. Im Bereich der Kreditwirtschaft hieß die entsprechende Lösung SWIFT/DTA. Die voranschreitende Internationalisierung und globale Verflechtung der Märkte und Geschäftsbeziehungen zwingen die Kreditwirtschaft jedoch eine branchenübergreifende strukturierte EDI-Infrastruktur aufzubauen. Banken können und werden mit EDIFACT, einen speziellen EDI-Standard im Zahlungsverkehr, die Rolle des Informationsbeschaffers, Informationsweiterleiters und Informationskonzentrators für den für eine intakte Warenwirtschaft notwendigen Finanzstrom übernehmen und ihre Aufgaben vom reinen

---

[33] Die NASA (http://www.nasa.com) nutzt seit Februar 1995 ein EDI-Softwareprodukt von der Fa. Premenos Cors. um ihre Beschaffungen mittels EDI über das Internet durchzuführen [Mes95].

Zahlungsausführenden hin zum Informationsprovider erweitern, neben weiteren hierdurch möglichen Service-Dienstleistungen in der Kunde/Bank-Beziehung.

Der flächenübergreifende Einsatz von EDI in der Kreditwirtschaft wird nach Ansicht von Thomas Egner (Bundesverband Deutscher Banken e.V.) noch einige Zeit in Anspruch nehmen. Bisher sieht er, daß die Entwicklung von EDIFACT als spezieller EDI-Standard im Finanzbereich augenblicklich das Experimentierstadium verläßt und sich am Markt etabliert [Egn96].

8.2 "TeleCounter"- als Prototyp

Im Forschungsprojekt "TeleCounter[34]" wird ein innovatives, zukunftsoffenes und interaktives Telematiksystem für das Segment der Klein- und Privatkunden (Konsumenten, Retailkunden) dargestellt. Ein Teilbereich des TeleCounter-Konzepts dient der Abwicklung des elektronischen Zahlungsverkehrs privater Kunden auf der Basis eines standardisierten Nachrichtenaustausches im Bankenbereich. Beim dargestellten Pilotprojekt der St. Gallener Hochschule wurde auf vorhandene Möglichkeiten zurückgegriffen, um ein modernes, den Bedürfnissen der privaten Kunden entsprechendes Zahlungsverkehrssystems zu implementieren. Das Pilotprojekt wurde in Zusammenhang mit zwei schweizerischen Großbanken und verschiedenen in der Telekommunikation tätigen Firmen durchgeführt. Unter der Verwendung von UN/Edifact-Protokolle, die weitverbreitet im internationalen Raum und branchenunabhängig sind, wird die Abwicklung des elektronischen, schweizerischen Zahlungsverkehrs privater Kunden über ihre Finanzdienstleister prototypisch dargestellt.

Die EDIFACT-Nachrichten verknüpfen dabei Basisdienstleistungen der Kreditinstitute wie z. B. Überweisungen, Zahlungsanweisungen, Daueraufträge und Lastschriften mit dem Kunden. Ohne im einzelnen auf die Entwicklung des Zahlungsverkehrsprototypen einzugehen, soll doch kurz das Resultat der Forschungsentwicklung dargestellt werden. Der Prototyp demonstriert, wie ein PC-Client mit einem benutzerfreundlichen graphischen Interface EDIFACT-Nachrichten durch verschiedene MHS-Systeme zu dem entsprechenden Kreditinstitut weiterleitet. Das System ist multibankfähig. Die EDIFACT-Nachrichten können

---

[34] Vertieft wird dieser Ansatz von Zimmermann „Telecounter: A case study on integration of private households in telematic services“ (http://www-iwi-unisg.ch/iwi4/cc/tc/hoit94.html).

aufgenommen und ausgeführt werden. Der elektronische Informationsservice für das Electronic-Banking basiert auf einem WWW-Server. Der Prototyp unterstützt aufgrund des EDIFACT-Nachrichtenaustausches den elektronischen Zahlungsverkehr, wobei das Clearing, d.h. die eigentliche finanzielle Verrechnung auf der Seite der Kreditinstitute bleibt [Zim95].

9. Internet-Lösung für den Zahlungsverkehr

9.1 CyberCash's Secure Internet Payment

Die Firma CyberCash Inc.[35] bietet, als eine der ersten Unternehmen, eine „real-time, end-to-end online payment"-Lösung für das Internet.

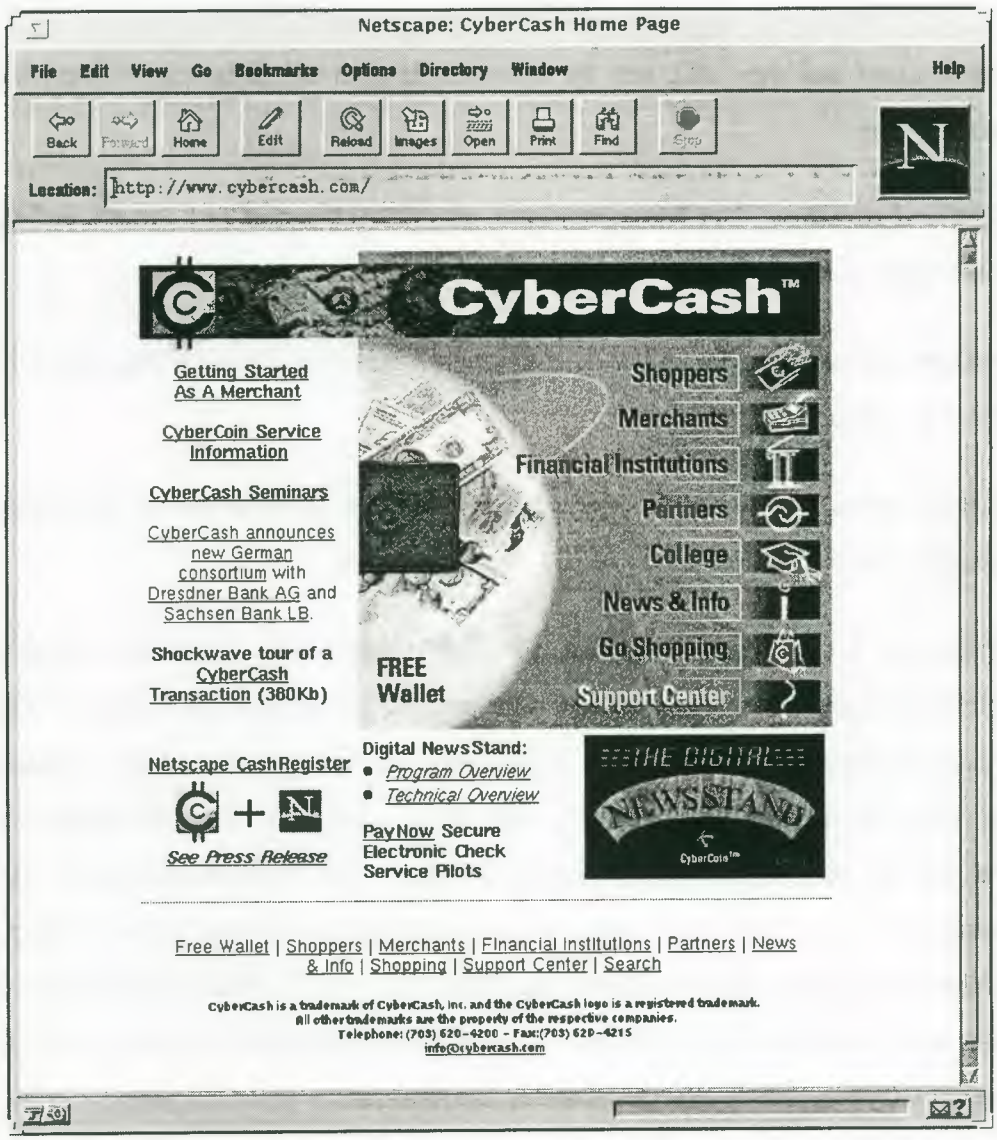

Abbildung 18: Homepage von CyberCash

[35] http://www.cybercash.com

9.1.1 Die Software

Die ***CyberCash-Wallet*** ist die Software für eine elektronische Geldbörse, die auf dem PC des Anwenders installiert wird. Sie kann kostenlos direkt von den Web-Seiten von CyberCash oder von den an das CyberCash-System angeschlossenen Banken und Händlern heruntergeladen werden (verfügbar für Windows 3.1X und Windows 95/NT). Diese Software bildet das Anwender-Interface für den „CyberCash Secure Internet Payment Service".

Mit dem Wallet[36] auf dem PC, hat der Internet-Shopper die folgenden Möglichkeiten der Online-Bezahlung:

1. ***Credit Card payments***; Der Anwender kann mit VISA, MasterCard, American Express und Discover Card sicher im Internet bezahlen.

2. ***CyberCoin payments***; Mit CyberCoin payments ist es möglich Beträge ab 25 Cents zu bezahlen (siehe unten).

3. ***Electronic check payments***; Geldaustausch über das Internet durch ein elektronisches Scheck-System (siehe Kap. 5.2).

Diese freie und kostenlose Verteilung der CyberCash-Wallet bietet für an das System angeschlossene Händler ein großes Potential möglicher Kunden, die schnell und einfach Waren kaufen können, die auf einer Web-Seite offeriert werden. Nach Installation der Software arbeitet die CyberCash-Wallet mit allen wichtigen Web-Browsern zusammen. Während des kurzen Installationsvorgangs vergibt der Verbraucher eine persönliche Identifikationsnummer und richtet seine existierenden Kreditkarten für die Wallet ein. Um beim Online-Shopping zu bezahlen, muß der Anwender lediglich die Schaltfläche „Bezahlen mit CyberCash" anklicken, die auf den Web-Seiten des Händlers angezeigt wird. Daraufhin öffnet sich die CyberCash-Wallet des Kunden automatisch.

Wie in der realen Welt, in der der Kunde im Geschäft zum Bezahlen sein Portemonnaie hervorholt, kann der Verbraucher nun aus seiner virtuellen Geldbörse, der CyberCash-Wallet, auswählen, ob er mit Kreditkarte oder direkt mit CyberCoins bezahlen möchte.

---

[36] Wallet ist das englische Wort für Brieftasche.

Das ***Cash-Register***, auch Secure Merchant Processing System (SMPS) genannt, ist ein Softwarepaket, das von CyberCash den Händlern zur Verfügung gestellt wird. Das Cash-Register wird auf dem Web-Server des Händlers installiert. Es kommuniziert sowohl mit der CyberCash-Wallet des Kunden als auch mit dem CyberCash-Gateway-Server (siehe unten). Prinzipiell ist das Cash-Register vergleichbar mit einem konventionellen POS-System (Point-of-Sale), das aber über spezielle Anpassungen für das Internet verfügt. Außerdem erlaubt es auch eine Nutzung durch mehrere Online-Händler gleichzeitig, z. B. im Rahmen einer virtuellen Shopping-Mall.

Das Cash-Register autorisiert Transaktionen und erstellt elektronische Bestätigungen. Neben der Gewährleistung sicherer Kreditkartentransaktionen stellt das Cash-Register dem Händler wichtige administrative Funktionalitäten zur Verfügung:

- manuelle Abwicklung von Kreditkartentransaktionen;
- editierbare Statusberichte zu erfolgten Transaktionen;
- Datenbankfunktionalität zur Unterstützung der Buchhaltung.

Das Cash-Register macht es zudem möglich, Bestellungen über Telefon, Fax oder Email zu bearbeiten. Somit steht den Händlern ein Progammpaket zur Verfügung, das alle Kreditkartentransaktionen abdeckt, bei denen die Kreditkarte nicht körperlich vorliegt.

Wichtig ist, daß das Design des Cash-Registers erlaubt:

- mehrere parallele Transaktionen zu bearbeiten, wenn das Geschäft des Händlers wächst;
- eine leichte Integration in die Web-Site des Händlers durchzuführen, ohne das System des Händlers in ein unübersichtliches und unflexibles Durcheinander von Applikationen zu verwandeln.

Das Cash-Register ist für Windows NT und alle gängigen UNIX-Systeme verfügbar. Die Anbindung an bestehende Web-Angebote erfolgt via CGI. So kann sie leicht den individuellen Bedürfnissen des Händlers angepaßt werden. Alle CGI-Scripts, die für den Datenaustausch zwischen dem Cash-Register und dem Webserver eingesetzt werden, sind in der Programmiersprache PERL geschrieben.

Der ***CyberCash Payment Gateway Server*** ist die Soft- und Hardware, mit der sichere Verbindungen zwischen den Händlern und ihren Kunden im Internet sowie den Banken/Kreditkartenorganisationen mit ihren bestehenden Netzwerken gewährleistet werden. Für die Banken/Kreditkartenorganisationen sehen CyberCash-Transaktionen genau wie traditionelle POS-Vorgänge aus. Der Payment Gateway Server bietet Firewall-Schutz, die Übersetzung von Nachrichten zwischen Internetprotokollen und den Datenstandards der Kreditwirtschaft sowie die Pflege und Authentizität der CyberCash-Wallet-IDs.

9.1.2 Die Sicherheit des CyberCash Systems

9.1.2.1 Die Registrierung

Beim ersten Start der Wallet-Software wird der Nutzer aufgefordert, eine Wallet-ID, seine Email-Adresse und eine Verifikations-ID sowie seine Kreditkartendaten einzugeben. Anschließend wird der Nutzer gebeten, ein Paßwort festzulegen. Mit diesem Paßwort wird die Wallet vor unberechtigtem Zugriff geschützt. Außerdem werden mit dem Paßwort alle zuvor eingegebenen Wallet-Daten verschlüsselt.

9.1.2.2 Die Verschlüsselung

Sämtliche Kommunikation zwischen der Wallet des Kunden, dem Cash-Register des Händlers und dem CyberCash-Gateway erfolgt über das Internet durch das Standard-Protokoll HTTP. Wenn Informationen zum Händler und von dort zum CyberCash-Gateway übertragen werden, erfolgt eine automatische Verschlüsselung der Daten durch die Wallet des Kunden. Dazu wird die Verschlüsselungstechnologie DES (Data Encryption Standard) mit 56-Bit-Schlüssel eingesetzt. Der Schlüssel ist für jede Transaktion einzigartig und wird vor dem Transport mittels RSA unter Verwendung von 1024-Bit-Schlüsseln kodiert. Diese Verschlüsselungstechnologie stellt zur Zeit die sicherste Methode dar, die von der US-Regierung für den Export freigegeben ist.

9.1.2.3 Speicherung der Daten

Bei Erhalt der vom Kunden bestätigten Bestell- und Zahlungsinformationen fügt das Cash-Register des Händlers dessen Identifikationsmerkmale hinzu und leitet die gesamten Daten an den CyberCash-Gateway-Server weiter. Die Verschlüsselung erfolgt analog zum Schutz der

Daten bei der Übertragung vom Kunden zum Händler. Im Unterschied zu konventionellen Kreditkartentransaktionen sieht der Händler die Kreditkartennummer nicht.

Das CyberCash-Gateway speichert keine sensitiven Daten von Kunden oder Händlern. Statt dessen werden alle beim Gateway zur Verifizierung von Transaktionen benötigten Daten nach einem Hash-Algorithmus geprüft. Es ist nicht möglich, aus diesen kodierten Daten wieder die ursprünglichen Informationen zu erzeugen. Um die Gültigkeit und Authentizität von Daten zu ermitteln, werden diese ebenfalls verschlüsselt und mit den gespeicherten Hash-Werten verglichen. Sensitive Informationen, die vom Kunden zum Händler gesendet werden, sind mit dem sitzungsabhängigen DES-Schlüssel abgesichert. Diese Daten können beim Händler nicht dekodiert werden. Dem Händler sind nur die für ihn relevanten Bestellinformationen des Kunden zugänglich. Die Software des Händlers ergänzt die Nachricht lediglich um eigene, wiederum verschlüsselte Zahlungsinformationen und sendet das Paket zum Gateway.

9.1.2.4 Betragslimitierung

Aus Sicherheitsgründen werden alle Daten und Informationen über Transaktionen oder Transaktionsschritte nur über einen begrenzten Zeitraum vorgehalten. Außerdem können für jeden Konsumenten maximale Beträge festgelegt werden, die der Nutzer auf die Wallet laden bzw. ausgeben kann. Damit kann sich der Kunde bei Fehlbedienung oder Unvorsichtigkeit vor hohen Verlusten schützen.

9.1.2.5 Buchführung

Die CyberCash-Wallet des Verbrauchers enthält ein Logbuch, in das alle Transaktionen automatisch eingetragen werden. Beim Händler werden alle Transaktionen in einem Transaktionslogbuch des Cash-Registers erfaßt. Es ist möglich, Transaktionen gezielt abzufragen und individuell oder nach Kreditkartentyp (EuroCard/MasterCard, Visa, AMEX, usw.) geordnet anzuzeigen.

9.1.3 CyberCoin payments

Im September 1996 erfolgte die Einführung von CyberCoin am amerikanischen Markt. Dieses neue und innovative Zahlungssystem ermöglicht Bartransaktionen über das Internet. Mit CyberCoin bietet sich Händlern die Möglichkeit, niedrigpreisige Produkte und Dienstleistungen im Web anzubieten. Beispiele hierfür sind Publikationen aller Art, Grafiken,

aktuelle Aktiennotierungen oder die Teilnahme an Online-Spielen. Für den Konsumenten wird Online-Shopping durch CyberCoin zum einfachen und bequemen Erlebnis. Möchte er ein Produkt mit CyberCoin bezahlen, so muß er lediglich die entsprechenden "Bezahlen"-Schaltfläche auf der Internetseite des Händlers betätigen. Das ist alles! Der ganze Vorgang nimmt nur wenige Sekunden in Anspruch und ist für den Kunden mit einem hohen Maß an Sicherheit verbunden (siehe oben). Beim CyberCoin-Verfahren lädt der Kunde seine elektronische Geldbörse, die Wallet, mit virtuellem Geld auf – online. Vor dem Einkauf definiert er das Höchstlimit und die Anzahl der zulässigen Transaktionen. Das „wirkliche" Geld wird jedoch niemals im PC des Kunden bzw. in seiner Wallet selbst gespeichert. Es verbleibt auf einem speziellen Bankkonto. Die CyberCoins haben somit lediglich eine „Nachweisfunktion" für das auf dem Bankkonto unterhaltene Guthaben (vgl. Ecash, Kap. 4.1).

9.1.3.1 Vorteile von CyberCoin

CyberCoin ist ein schnelles, bequemes und einfaches Verfahren für sichere Zahlungsleistungen über das Internet. CyberCoin ermöglicht sichere Transaktionen und eröffnet Händlern neue Möglichkeiten, Güter und Dienstleistungen im Internet anzubieten, die durch CyberCoin sofort bezahlt werden können. Der Internetnutzer verfügt mit dieser neuen Technologie über eine Softwarelösung, die ihm den Einkauf im Internet auf bequeme und sichere Art und Weise ermöglicht. Im Zuge der steigenden Akzeptanz von Kreditkarten- und Coin-Zahlungen im Internet erhalten die Online-Händler die Möglichkeit, ihre bislang als Marketingplattform genutzte Homepage zum vollwertigen Vertriebskanal auszubauen. Im Zusammenspiel mit der CyberCash-Wallet bietet dabei das Cash-Register, die virtuelle Registrierkasse, die Autorisierung und Abrechnung der im Internet erzielten Umsätze über die dem System angeschlossenen Banken.

9.1.4 Ablauf einer Kreditkartentransaktion

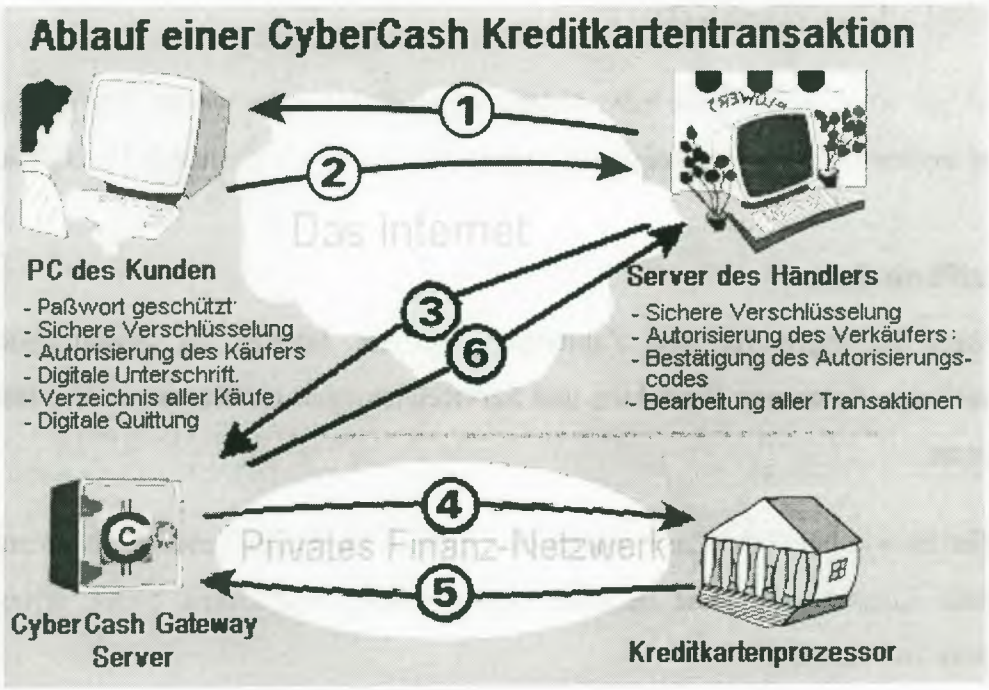

Abbildung 19: Ablauf einer Kreditkartentransaktion

1. Ein Konsument hat sich in einem elektronischen Warenhaus Produkte angesehen und sich dafür entschieden, etwas zu kaufen. Nach Eingabe der notwendigen Daten (Produktdaten, Lieferanschrift u. ä.) erhält er vom Händler eine Auftragsbestätigung.

2. Der Kunde betätigt die „Bezahlen"-Schaltfläche. Dadurch wird die CyberCash-Wallet-Software geöffnet. Der Kunde wählt aus seiner Wallet die Kreditkarte, die er für den Zahlungsvorgang benutzen möchte und schließt den Vorgang durch Anklicken einer entsprechenden Schaltfläche ab. Die Auftrags- und verschlüsselten Zahlungsdaten werden an den Händler weitergeleitet.

3. Der Händler erhält die Daten und separiert die Auftrags- von den verschlüsselten Zahlungsdaten. Mit seinem „private key" digital unterschrieben und verschlüsselt, werden die Zahlungsdaten an das Gateway von CyberCash weitergeleitet.

4. Das Datenpaket wird vom Gateway durch den Firewall geleitet und somit aus dem Internet herausgenommen. Dann werden die Informationen entschlüsselt und über die vorgegebenen Wege an den Kreditkartenprozessor weitergeleitet.

5. Es erfolgt eine Autorisierungsprüfung. Die Freigabe der Zahlung bzw. die Ablehnung wird an CyberCash zurückgeschickt.

6. CyberCash leitet die Freigabe bzw. Ablehnung an den Händler weiter. Von dort gelangt sie weiter an den Verbraucher. Der ganze Vorgang dauert durchschnittlich 15–20 Sekunden.

9.2 VeriFone GmbH

Um sichere Lösungen für den Zahlungsverkehr im Internet zu gewährleisten, bietet VeriFone[37] eine Reihe von Produkten und Serviceleistungen für Konsumenten, Händler und Betreiber an.

- ***vWallet*** ist wie bei CyberCash Wallet eine einfach zu handhabende Softwareanwendung, die dem Konsumenten eine bequeme und einfache Möglichkeit bietet, seine Internet-Einkäufe zu bezahlen.

- ***vPOS*** erfaßt Auftrags- und Zahlungsinformationen. Es kommuniziert mit vGate, um eine Autorisierung zu erhalten und verarbeitet die Zahlung. vPOS besitzt alle Funktionen eines POS-Zahlungssystems. Die Software stellt eine einfache Kunden-Zahlungsschnittstelle zur Verfügung, ermöglicht Kredite, Stornierung von Zahlungen, Zahlungsabwicklung, Gutschrift und liefert einen Zahlungsbeleg für den Kunden.

- Das ***vGate*** ermöglicht die sichere Weiterleitung der Transaktionen vom Internet-Händler an den Autorisierungshost, ohne diese zu verändern. Es verarbeitet alle Internet-Zahlungsprotokolle, alle internetspezifischen Sicherheitsprotokolle, die Umwandlung von Protokollen, sowie die direkte Autorisierung und Zahlungsabwicklung

Alle VeriFone-Produkte sind mit geprüften Sicherungssystemen basierend auf Public Key Verschlüsselungen ausgestattet. Dies garantiert die Vertraulichkeit und Integrität sowie die Bestätigung der Autorisierung durch die jeweiligen Parteien. Das SET-Protokoll wird voll unterstützt werden.

---

[37] http://www.verifone.com

10. Transaktionsformen in elektronischen Märkten

In diesem Kapitel werden die Transaktionsformen, die in elektronischen Märkten implementiert sind, untersucht. Mit dem Begriff „Transaktionen" sind alle Formen von Geschäftskontakten und -prozessen gemeint [Schmidt et al.95]. Elektronische Märkte besitzen die gleichen Funktionen (electronic shopping, business to business), die auch die klassischen Märkte besitzen [Kuhlen96], allerdings bedienen sie sich ausschließlich der Telematik. Schaut man sich die im Internet bereits vorhandenen Märkte näher an, so stellt man verschiedene Ausprägungsformen der Transaktionsfunktionen fest.

Viele „Online-Marktplätze" sind eigentlich nur eine Sammlung von einfachen Unternehmenspräsentationen, dabei werden die Unternehmen und ihre Dienstleistungen meist sehr kurz dargestellt. Die Betreiber solcher Marktplätze werben dabei um Kunden (Unternehmen, die sich online präsentieren möchten) mit dem Argument, daß sie durch die Präsentation im Internet eine neue Kundenzielgruppe ansprechen und daraus resultierend höhere Verkaufszahlen erzielen können. Die Marktplatzbetreiber vergessen dabei völlig (oder verschweigen es), daß dieses Medium ganz andere Marketingformen benötigt um tatsächlich auch eine Verkaufsförderung zu erzielen. Dementsprechend beschränken sich die Transaktionsform in diesen einfachen Online-Marktplätzen auf die Email-Funktion. Interessenten können über ganz normale Email oder über ein „Kontaktformular" mit dem Unternehmen in Kontakt treten. Viele der Unternehmen, die sich in einem Online-Markt präsentieren, besitzen selbst noch nicht einmal einen Internetanschluß und damit verbunden eine eigene Email-Adresse, so daß das Kontaktformular bzw. die Kontaktaufnahme meist über ein Faxgerät oder telefonisch weitergeleitet werden muß.

Eine Verbesserung, um mit einem Unternehmen in Kontakt zu treten oder etwas zu bestellen, bieten sogenannte Online-Bestellformulare. Sie sind meist nichts anderes als das Abbild der Offline-Bestellformulare wie man sie aus dem Versandhandel bereits kennt. Einige Unternehmen haben jedoch an diese Formulare einen virtuellen Warenkorb und eine Produktdatenbank angebunden. Dadurch hat der Kunde die Möglichkeit sich bestimmte Produkte anzeigen zu lassen und wie bei einem *normalen* Einkauf, die Ware in seinen Warenkorb zu legen. Ist der Kunde mit seinem Einkauf fertig, werden die von ihm in den Warenkorb gelegten Produkte automatisch in das Bestellformular eingetragen und der zu zahlende Betrag errechnet. Auf dem Formular muß der Kunde nur noch die

Rechnungsadresse, die Lieferadresse und die gewünschte Zahlungsart angeben. In den meisten Fällen verwenden die Serverbetreiber keinen Sicherungsmechanismus, um diese Daten verschlüsselt durch das Netz zu transportieren.

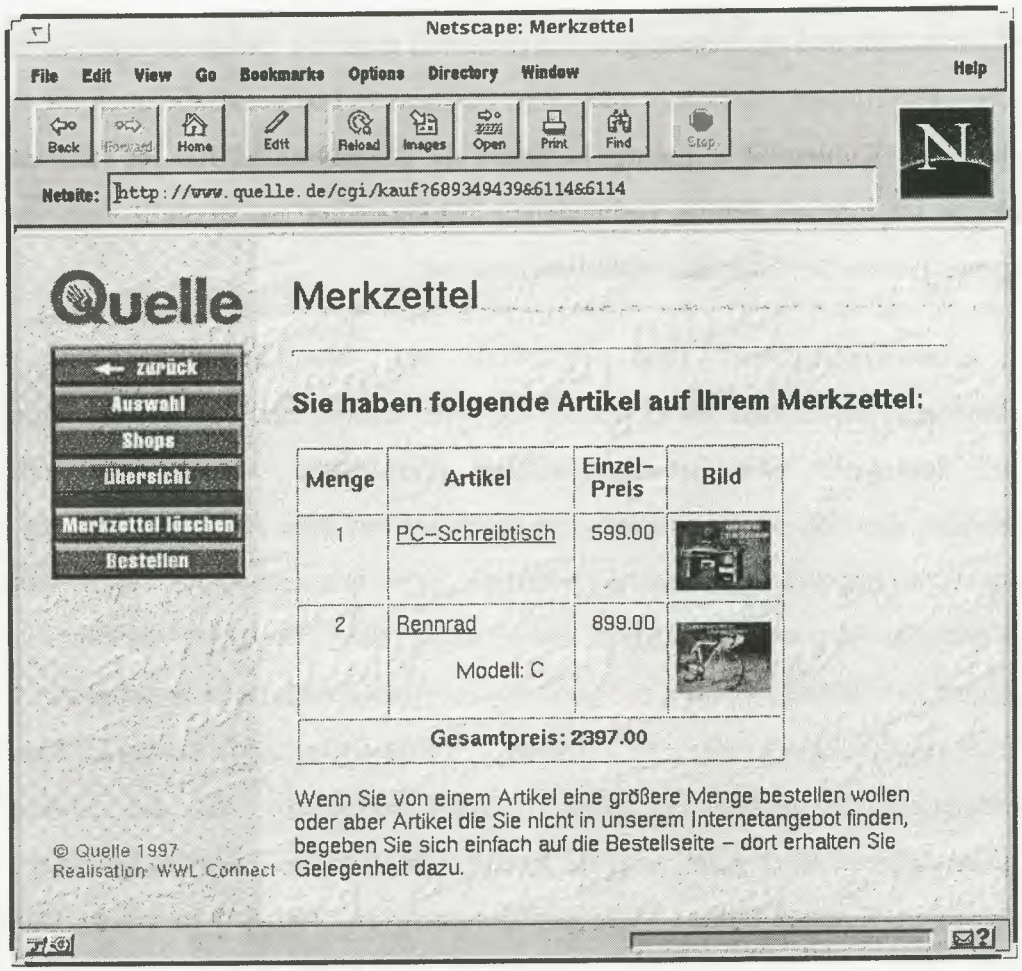

Abbildung 20: Warenkorb bzw. „Merkzettel“ von Quelle (http://www.quelle.de)

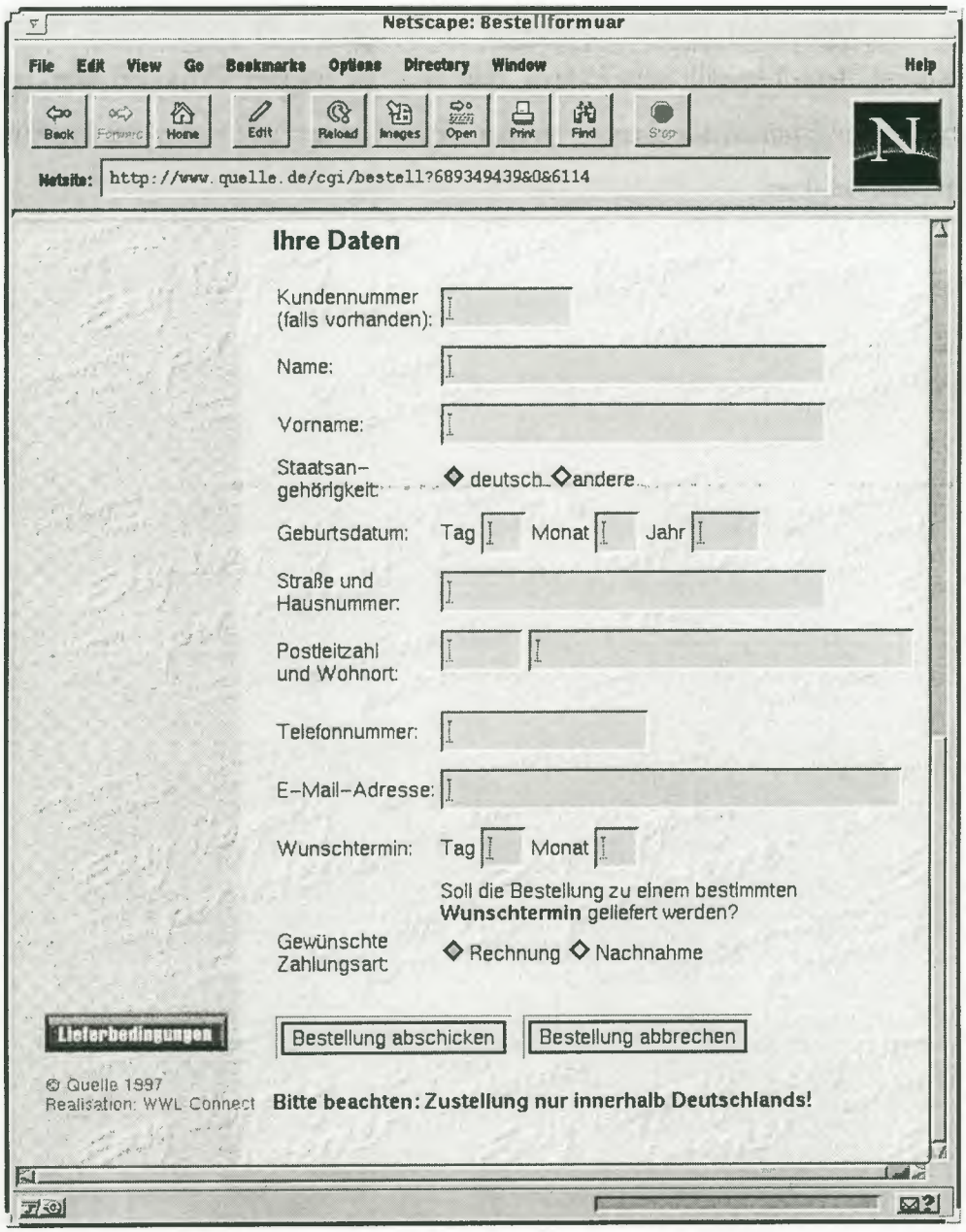

Abbildung 21: Der Kunde muß noch die Lieferadresse einfügen

Die Auswahl der Produkte durch die Verwendung einer Datenbank und die Bestellung der Ware mit Hilfe eines Online-Formulares ist die zur Zeit im Internet am weitesten entwickelte Transaktionsform. Auf diesem Gebiet wird sich jedoch in Zukunft einiges ändern. Denkbar wären Transaktionsformen bei denen die bestellte Ware gleich über Ecash, CyberCash, VeriFone oder ähnliche Systeme bezahlt würde. Diese echten „Internet-Business-Systeme" hätten dann auch den Vorteil, daß z. B. Kartenreservierungen für das Kino oder für ein Museum online möglich wären. Zudem ist vorstellbar den Einsatz von Sicherheits- und Zahlungssysteme Behördenanträge und deren Abwicklung über das Internet zu realisieren. Die

Schaffung und Integration solcher Internetanwendungen in die bestehenden elektronischen Märkte würden dann letztlich dazu führen, daß diese zu wahren virtuellen Marktplätzen mit allen notwendigen Transaktionsformen werden, und nicht nur wie bisher die Funktionen einer einfachen Mall besitzen.

11. Transaktionsformen im Online-Banking

Das Bankgewerbe befindet sich im Umbruch. Aktien- und Wertpapiergeschäfte erledigt der Kunde per Datenanschluß von Zuhause. Traditionelle Banken erhalten Konkurrenz von branchenfremden Kreditinstituten, die bessere Konditionen bieten. Ermöglicht wird dies durch den Einsatz unterschiedlicher Sicherheitskonzepte im Internet und durch die steigende Akzeptanz von Online-Diensten.

11.1 Online-Banking - mehr als nur Online-Kontoführung

Es ist nicht mehr selbstverständlich, daß Bankkunden ihre Finanzgeschäfte auch weiterhin bei traditionellen Banken abwickeln. Schon jetzt sind Trends erkennbar, daß Bankdienstleistungen zukünftig verstärkt von Netzbetreibern, Versandhäusern, Automobil- oder Multimedia-Konzernen angeboten werden. Etwa von Quelle[38] und Volkswagen[39], die bereits Banking-Angebote im Internet offerieren. "Wer die Netze hat, hat die Verbindung zum Kunden", so hat es Bill Gates einmal formuliert und dies sind hierzulande nicht typischerweise die Banken. Wettbewerber aus dem Non- und Near-Bankbereich stellen zudem ausgesprochen attraktive Konditionen, so daß sich viele Bankkunden überlegen, ob sie als Alternative zu einem Geldmarktfond für kurzfristige Anlagen ein Konto bei einer Bank aus der Automobil- oder Versandhausbranche wählen. Dort unterhaltene Guthaben unterliegen keinen Kursschwankungen, sind sofort verfügbar und verursachen keine Transaktionskosten. Das so ausgestattete Konto beispielsweise bei der VW-Bank könnte damit zur Meßlatte für attraktive Konditionen avancieren. Hinter den branchenfremden Banken stehen seriöse Firmen, die den gleichen strengen Normen des Bundesaufsichtsamtes für Kreditwesen unterliegen wie die klassischen Banken.

Für den deutschen Anleger scheinen die international ausgerichteten Finanzdienstleister, die bereits über Erfahrungen in globalen Datennetzen verfügen, eine interessante Alternative zu sein. Adressen[40] wie die Barclays Bank, Chase Manhatten, Bank of America, aber auch Banken, die bislang keinen bekannten Namen haben, wie die Mark Twain Bank, befinden sich im Internet und sind damit auch für hiesige Anleger erreichbar. Neben Wells-Fargo,

---

[38] Http://www.quelle-bank.de

[39] http://www.vw-online.de/vw_bank/

Aufhauser, Lombard Brokerage, Charles Schwab sind noch gut zwei Dutzend weitere Broker diesen Schritt gegangen und bieten ihre Leistungen über das Internet an - und zwar für hiesige Verhältnisse zu ungewöhnlich günstigen Konditionen. Einen kompletten Wertpapierumsatz, also Kauf- und Verkaufstransaktionen, gibt es bereits für unter acht Dollar, in Deutschland kosten vergleichbare Leistungen im günstigen Fall knapp 30 Mark. Ergänzt werden diese Online-Aktivitäten durch moderne Multimediaterminals, die fast einen Fullbankservice ermöglichen. So ist in Japan bereits die Kreditvergabe über Automaten möglich; der Vorgang dauert knappe 30 Minuten, inklusive Prüfung und Auszahlung über entsprechende Chipkarten. Es ist wohl nur noch eine Frage der Zeit, bis derartige Leistungen auch über das Internet angeboten werden.

Aufgeweckt von dieser rasanten Entwicklung, beginnt die deutsche Banken-Szene teils überlegt, teils unüberlegt mit ihren Internetaktivitäten. Nachdem fast jede größere Bank oder Institutsgruppe eine Direktbanktochter in verschiedensten Varianten gegründet hat, ist die nächste Gründungswelle im Gange. Diese findet im Internet oder kommerziellen Online-Diensten statt. Allerdings sind die bisher präsentierten Angebote - von wenigen Ausnahmen abgesehen - noch weit von einer virtuellen Bankfiliale entfernt. Erst ab Mitte 1997 ist mit echtem Transaktionsbanking zu rechnen.

Den deutschen Banken und Sparkassen ist offenbar bewußt, daß sich die Szenarien in der nächsten Zeit dramatisch verändern, und daß sowohl die Vertriebsstrukturen als auch das Kundenverhalten davon betroffen sein werden. Offenbar fehlen noch entsprechende Konzepte, wie auf diese Entwicklungen zu reagieren ist. Zusätzlich wird der Anpassungsprozeß durch unflexible Strukturen und nur schwer reversible Rahmenbedingungen erschwert. Direktbanken haben derzeit bestenfalls die Chance, als Zweitbank zu fungieren. Eine Hürde, die hiesige Unternehmen insbesondere im Wettbewerb mit der amerikanischen Konkurrenz oder den branchenfremden Anbietern von Finanzdienstleistern benachteiligt.

Mit Blick auf die enormen Veränderungen, denen sich die Banken ausgesetzt sehen, ist es daher sehr verwunderlich, welch geringes Leistungsspektrum die Institute ihren Kunden derzeit im Bereich des Internet-Bankings anbieten. Selbst im Vergleich zum Homebanking via T-Online, das meist nur Grundfunktionen der traditionellen Kontoführung ermöglicht,

---

[40] Einen Überblick über die URL´s der Banken bietet Kapitel 11.4

schneiden die Service-Leistungen des Internet-Bankings schlechter ab. Kaum eine Bank bietet bislang einen vollen Kontoführungsdienst, geschweige denn die Möglichkeit, Wertpapiergeschäfte online zu tätigen. Banken, die bereits echte Transaktionen über das Internet zulassen, setzen im Grunde genommen nur über einen Gateway-Server auf das altbewährte T-Online auf.

Die Bequemlichkeit, Geschäfte von jedem beliebigen Ort aus zu tätigen, kann nicht der einzige Mehrwert sein, zumal der Zugang zum Internet selbst für technisch versierte Menschen nicht immer einfach ist. Auch die aktuell entbrannte Diskussion über die Unsicherheit von Homebanking läßt so manchen Anleger zweifeln; nicht wenige Kunden greifen dann doch lieber zum Telefon oder nutzen das Faxgerät, aber eine ausgereifte Lösung des Sicherheitsproblems scheint durch die Einführung des Homebanking Computer Interface (HBCI)[41] in Sicht.

11.2 Mehr Sicherheit im Homebanking durch „Homebanking Computer Interface (HBCI)"

Die deutschen Banken werben mit einem neuen Sicherheitsstandard für das Internet. Noch in diesem Jahr soll ein Sicherheitsstandard für Geld-Transaktionen am PC eingeführt werden, der mittels einer "elektronischen Unterschrift" die Kundenkonten zuverlässig gegen Hackerangriffe schützen soll.

Aufmerksamkeit erregte das Homebanking Computer Interface (HBCI), das auf der Cebit 1997 der Öffentlichkeit vorgestellt wurde. Dieses Sicherheitskonzept wurde vom Zentralen Kreditausschuß der deutschen Geldinstitute (ZKA)[42] entwickelt und soll die gemeinsame Plattform für alle Banken und Sparkassen bilden, die Bankleistungen in offenen Netzen

---

[41] http://www.softlab.de/german/hbci/hbci.html

[42] Der Zentrale Kreditausschuß, im Jahre 1936 zur Festsetzung der Zins- und Provisionssätze und zur Regelung des Wettbewerbs zwischen den Kreditinstituten gegründet, hat nach Aufhebung der Zinsverordnung 1967 nicht mehr die frühere Bedeutung. Dem ZKA gehören die Spitzenverbände des Kreditgewerbes (Deutscher Sparkassen- und Giroverband e. V., Bonn, Verband öffentlicher Banken e. V., Bonn, Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V., Bonn, Bundesverband deutscher Banken e. V., Köln, Verband der Gemeinwirtschaftlichen Geschäftsbanken VGG, Bonn) an; die Geschäftsführung wechselt in jährlichem Turnus unter diesen Verbänden. Der ZKA befaßt sich heute mit den das Kreditgewerbe gemeinsam berührenden Fragen, hat jedoch aus kartellrechtlichen Gründen nur noch beratende Funktion.

anbieten und gleichzeitig einen massiven Schutz vor Hackern und Viren bieten wollen. Im Vordergrund der Überlegungen standen die Mehrfachbankfähigkeit und eine einheitliche Datenbank für Einwahladressen, so daß Kunden auch mehrere Bankverbindungen ohne Umstände ansteuern können. Die Kunden könnten damit auf T-Online und im Internet ihren Finanzstatus bei verschiedenen Banken mit einem einzigen Tastendruck abrufen. Mit dem neuen Sicherheitsstandard könnten dann nicht nur Daueraufträge und Überweisungen am PC erledigt werden, auch die Depotverwaltung und später auch die Kreditvergabe sollten von zu Hause abgewickelt werden können. Durch eine elektronische Unterschrift wird die Sicherheit gegen Manipulation gewährleistet. Gegen unberechtigte Einsichtnahme schützen jeweils entsprechende Verschlüsselungsverfahren.

Nachrichten über Einbruchsversuche in Netzwerk-Computer häuften sich in den vergangenen Monaten. Glaubt man den Verantwortlichen, so ist es bisher noch zu keinem Fall von elektronischen Bankeinbrüchen gekommen. Die Branche hat und hatte offenbar keine Probleme mit Homebanking via T-Online, obwohl die Schwachstellen des Homebankings bekannt sind. Denn tatsächlich werden die Daten unverschlüsselt über die Telefonleitungen verschickt und könnten auch abgefangen werden - es muß nur der richtige Zeitpunkt abgepasst werden. Unbestritten ist auch, daß es technisch möglich ist, die elektromagnetischen Strahlen eines PC-Bildschirms einzusehen und so die persönliche Identifikationsnummer (PIN) und die Transaktionsnummer (TAN) auszuspionieren, die den Zugang zum Konto des Besitzers ermöglichen. Letzten Endes werden über T-Online jedoch überwiegend Kleinbeträge transferiert, die den hohen technischen Aufwand des Hackens und das damit verbundene Strafrisiko in keiner Weise rechtfertigen würden. Zudem bleibt das Geld ausschließlich im Bankensystem, so daß stets nachvollzogen werden kann, wohin es transferiert wurde. Bankberater sind darüber hinaus gehalten, ihren Kunden grundsätzlich die Verhaltensweisen im Umgang mit PIN und TAN zu erläutern.

Aufgrund der boomhaften Entwicklung des Internets werden Homebanking-Anwendungen nicht nur bei T-Online, sondern zunehmend im World Wide Web angeboten. Um auf dieser Welle mitsurfen zu können, bieten manche kommerziellen Dienste den Nutzern an, die bereits vorhandenen T-Online-Angebote aus dem Internet heraus zu nutzen. Die Homebanking-Funktionen der Banken und Sparkassen werden dabei über ein Internet-T-Online-Gateway und eine Formaterkennung bereitgestellt, so daß der Kunde nicht unmittelbar mit seiner Bank, sondern über die Internet-Seiten des Dienstanbieters kommuniziert. Mit Hilfe dieser Technik

ist es möglich, das für T-Online geschaffene Electronic-Banking System GenoDirekt[43] ohne Software-Anpassung über einen World-Wide-Web-Server ans Internet anzubinden. Solange derartige Internet-T-Online-Übergänge von seriösen Firmen im Auftrag von Banken betrieben werden und die Kommunikation über das Internet zwischen Service-Anbietern und Kunden ausreichend abgesichert ist, erscheint das zusätzliche Risiko dieser Praxis vertretbar.

11.3 Beispiele von Banken im Internet

Fast alle großen deutschen Banken sind derzeit im Internet vertreten. Ihr Internetangebot beschränkt sich dabei in den meisten Fällen auf das einfache Anbieten von Informationen, die in der Regel aus der Beschreibung des Dienstleistungsangebotes der Bank bestehen. Einige Banken gehen auch einen Schritt weiter, sie stellen aktuelle Börseninformationen, Anlagetips, Immobilienangebote, etc. zur Verfügung. Die Möglichkeit das eigene Girokonto oder das Aktiendepot zu verwalten, Ankaufs- und Verkaufsorder über das Internet zu geben ist derzeit nur bei wenigen Banken vorhanden. Was gänzlich bei allen noch fehlt ist ein standardisiertes Internet-Zahlungssystem, lediglich die Deutsche Bank wird gegen Ende dieses Jahres einen Pilotbetrieb mit Ecash durchführen. Der Pilotbetrieb ist für 6 Monate vorgesehen.

11.3.1 Bank24 und Deutsche Bank

Die Firewalls der Bank24 und der Deutschen Bank wurden von zwei anerkannten Prüfungsgesellschaften testiert, so daß man bei der Deutschen Bank davon ausgeht, daß ein Zugriff auf die Kontendaten in den Systemen der Bank ausgeschlossen sei. Bei der Kontaktaufnahme mit der Bank über das Internet wird diese automatisch identifiziert, vorausgesetzt der Client benutzt einen Browser, der die Programmiersprache Java unterstützt. Die Identifizierung geschieht mit Hilfe eines Schlüsselpaars, das von der amerikanischen Firma VeriSign[44] zertifiziert ist. Dadurch kann der Kunde sicher sein, daß alle Daten, die er empfängt, auch von seiner Bank stammen. Die bei der Übermittlung von sensiblen Kundendaten verwendeten Verschlüsselungen beruhen auf international anerkannten Algorithmen, die im Bankbereich etabliert sind (RSA, SSL).

---

[43] http://www.genodirekt.de

[44] http://www.verisign.com

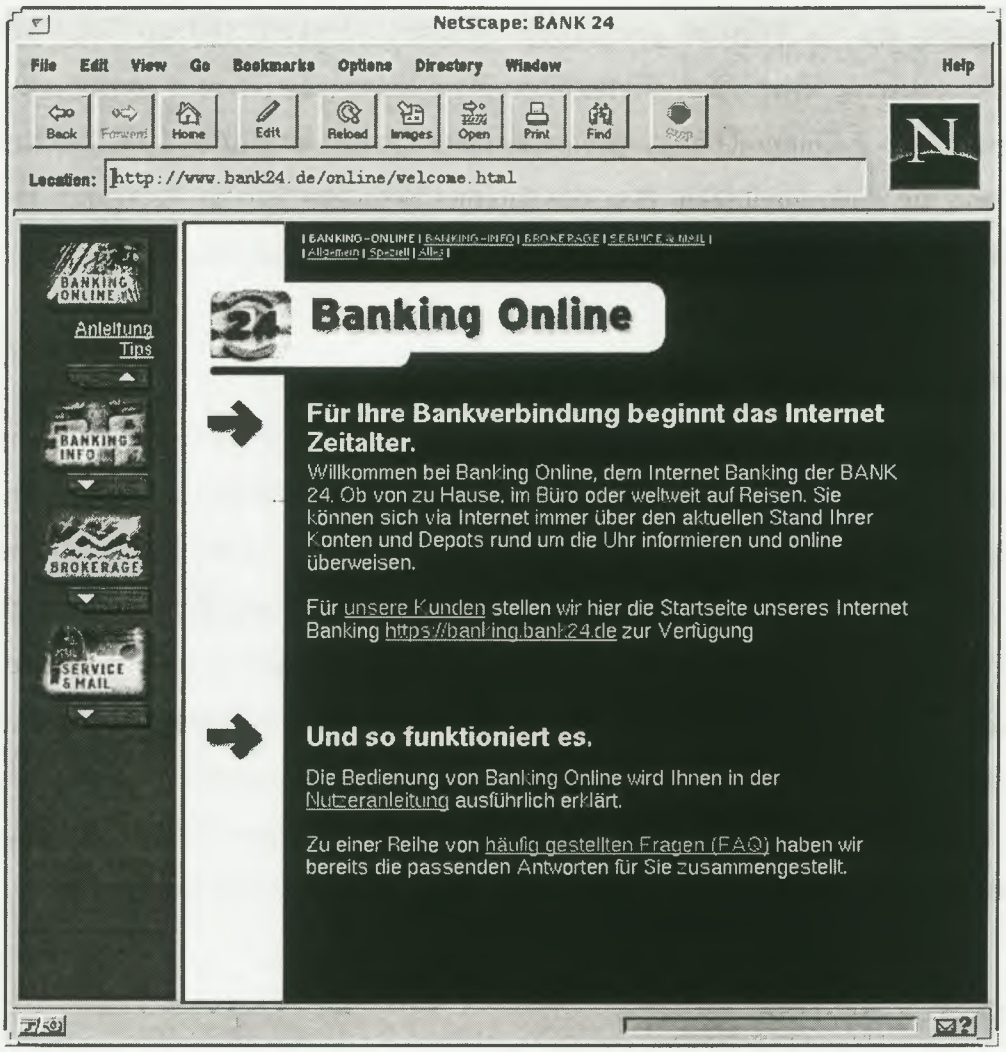

Abbildung 22: Homepage der Bank24

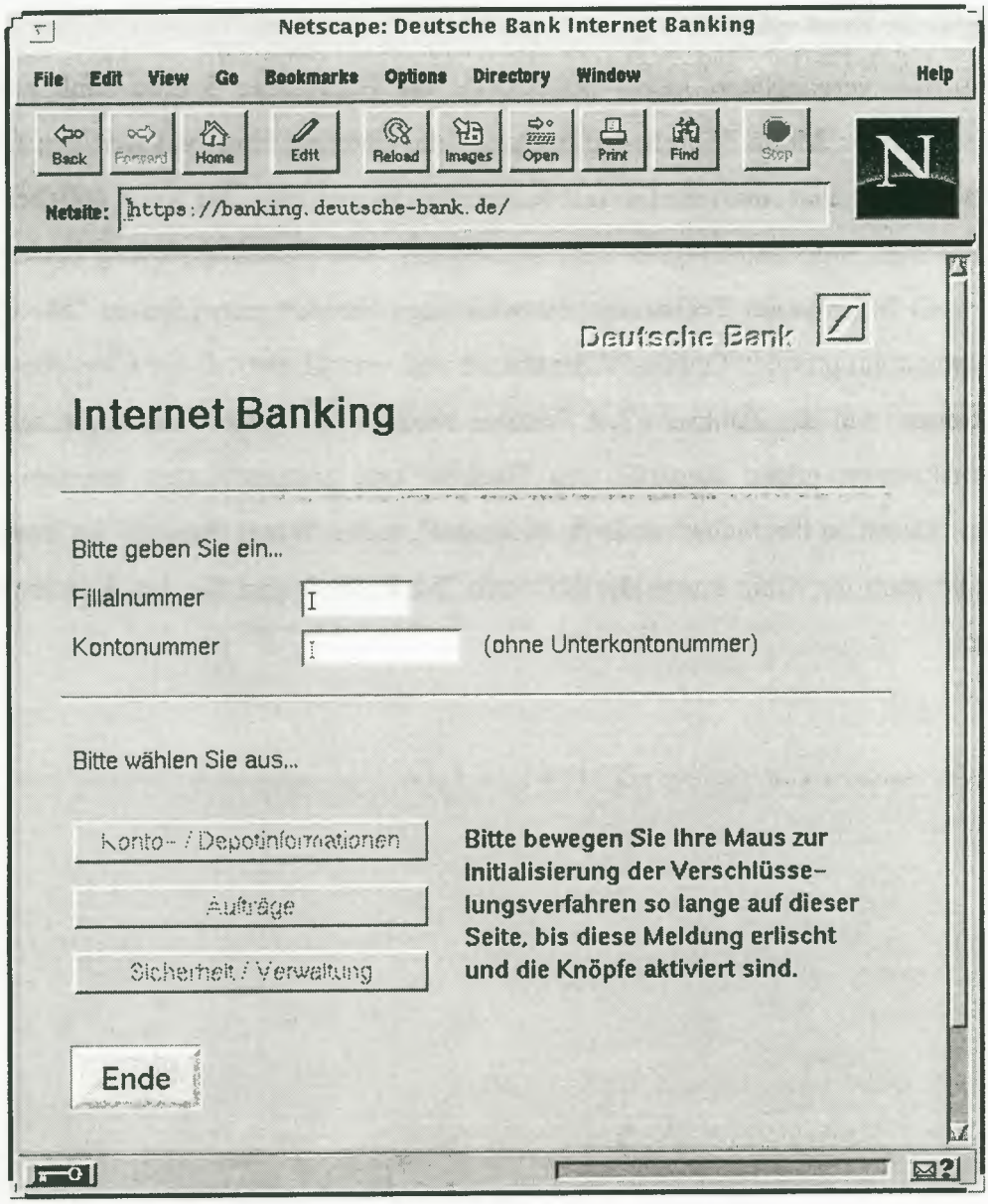

Abbildung 23: Einstiegsseite zum Internetbanking der Deutschen Bank

Außerdem wird vor und nach der Übertragung der Daten ein elektronischer "Fingerabdruck" erzeugt. Der Vergleich der beiden Fingerabdrücke stellt sicher, daß während des Transfers keine Manipulation stattgefunden hat. Damit sei die Integrität der Daten garantiert, so die Verantwortlichen der Deutschen Bank. Auf einer letzten Stufe kommen dann die bewährten PIN- und TAN-Verfahren zum Einsatz. Diese werden bereits im PC des Kunden verschlüsselt und so zur Bank übertragen. Damit soll auch das unbefugte "Anzapfen" von Leitungen ausgeschlossen werden.

11.3.2 Sparda-Bank e.G.

Schon im Juli vergangenen Jahres präsentierte die Hamburger Sparda-Bank e.G.[45] ihren Kunden unter dem Motto "Sparda-NetBanking" die Führung eines vollwertigen Girokontos im Internet an. "Sicher, multimedial und kostengünstig und ohne die sonst üblichen TAN's", so Heinz Wings, Vorstandsmitglied der Sparda-Bank. Die Sicherheitslösung basiert auf dem von der ESD Information Technology Entwicklungs GmbH[46] entwickelten "Me-Chip". Als Zusatzelement am privaten Online-PC bearbeitet und verschlüsselt dieser Chip alle relevanten Transaktionen. Auf der Bankseite hat Siemens Nixdorf das System durch ein mehrstufiges Sicherheitskonzept gegen Angriffe von Hackern und unberechtigten internen Zugriffen gesichert. "Damit ist die Sicherheitskette lückenlos", meint Wings. Sowohl der Internetkonto-Service als auch der Chip sowie die Software "MeWallet" sind für den Kunden kostenlos verfügbar.

[45] http://www.sparda-hh.de

[46] http://www.esd.de

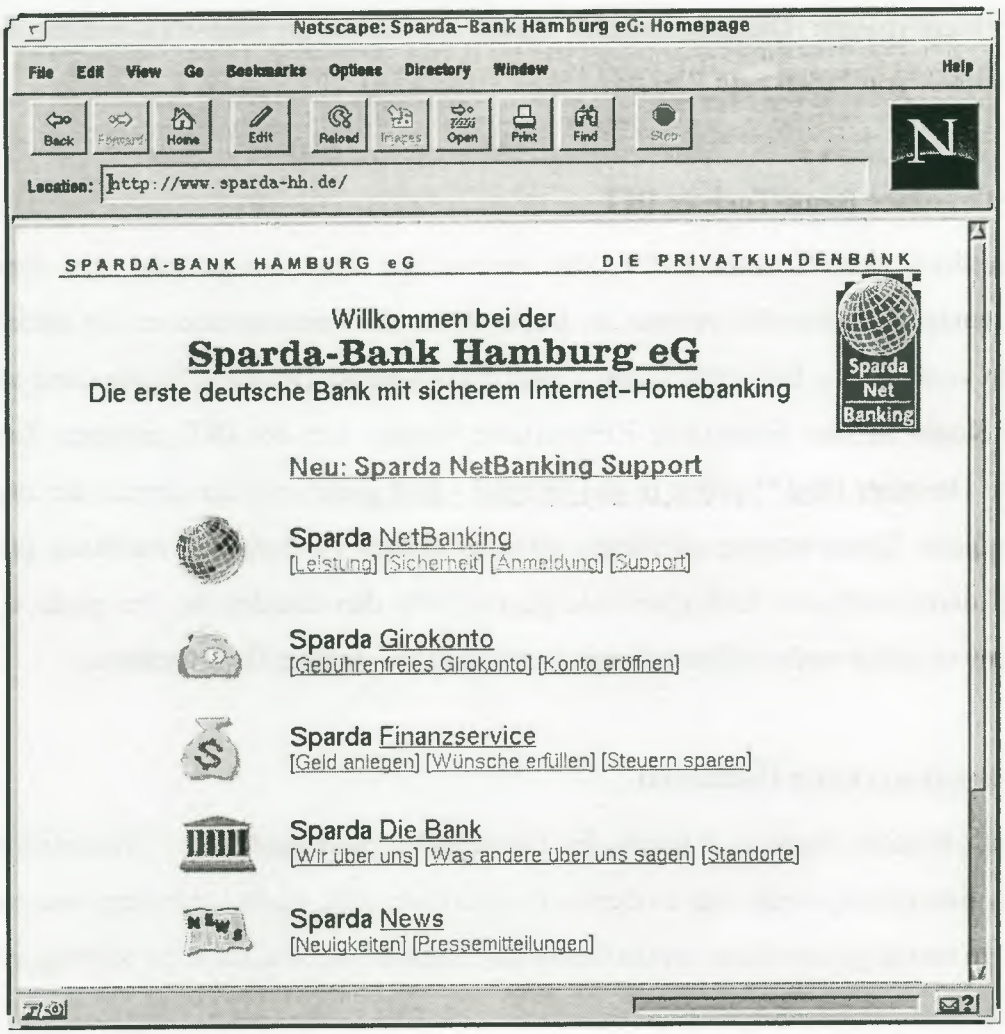

Abbildung 24: Homepage der Sparda Bank Hamburg e.G.

11.3.3 Privatbankhaus Gries & Heissel

Seit Ende August bietet das Berliner Privatbankhaus Gries & Heissel[47] einen weltweit verfügbaren Onlinebanking-Service. Die Realisierung aller erforderlichen Sicherheits- und Verschlüsselungstechniken erfolgt kundenseitig ausschließlich auf der Basis standardisierter Software, so daß dieser weder spezielle Hard- und Software benötigt. Das via Internet nutzbare Leistungsspektrum der Bank umfaßt verschiedene Abfragen von Konten und Depots inklusive eines Gesamtvermögensstatus, eine komfortable Oberfläche für das Wertpapiergeschäft, die Erledigung von Überweisungen und Lastschriftaufträgen sowie

[47] http://www.guh.de

weitere banktypische Dienstleistungen. Auch bei Gries & Heissel kommen anerkannte Sicherheits-Algorithmen zum Einsatz.

11.3.4 Dresdner Bank-Tochter DIT

Die Dresdner Bank-Tochter DIT[48] läßt bereits seit über einem Jahr den Erwerb von Investmentanteilen über das Internet zu. Dabei sehen die Verantwortlichen das höchste Risiko in einem vom Timing her ungünstigen Verkauf der Anteile. Das Geld würde dann stets direkt auf ein Konto fließen. Eventuelle Kursverluste würden von der DIT getragen. Zuletzt ging auch die Dresdner Bank[49] selbst in das Internet - und gleich mit der Option der interaktiven Orderaufgabe. Dabei werden allerdings lediglich Orders via Email an die Bank geleitet und dort auf deren sachliche Richtigkeit hin geprüft. Für den Kunden ist dies mehr eine Black Box, denn er erhält weder Informationen über Konto- noch über Depotbestände.

11.3.5 Stadtsparkasse Dortmund

Als erste deutsche Sparkasse bietet die Dortmunder Stadtsparkasse[50] Transaktionsbanking über das Internet an, wenn man es denn so bezeichnen will. Nach jeder Kundenorder ruft ein Berater an und fragt der Sicherheit halber noch einmal nach, ob alles seine Richtigkeit hat.

11.3.6 Online-Brokerage als Mehrwert auf der Datenautobahn

Als Trendsetter für Homebanking erweisen sich hingegen die verschiedenen Onlinebroker, die ihren Service fast ausschließlich über das Internet anbieten. Von der Anwerbung des Kunden, dem Vertragsabschluß, über die Leistungserstellung in Form von Abwicklung und Ausführung von Orders, also den An- und Verkauf, bis hin zur Berichterstattung über den Erfolg oder Mißerfolg geschieht faktisch alles nur noch online. Nach einer erst kürzlich von Forrester Research, Cambridge, veröffentlichten Studie, werden derzeit bereits knapp 800.000 Wertpapierdepots weltweit via Onlinebrokerage verwaltet, was schätzungsweise ein Prozent aller Depots ausmachen dürfte. Bis zum Jahr 2000 wird eine Verdoppelung erwartet.

---

[48] http://www.dit.de

[49] http://www.dresdner-bank.de

[50] http://www.stadtsparkasse-dortmund.de

11.3.7 Dresdner Bank und Sachsen LB

Zur Einführung eines sicheren Bezahlsystems für das Internet haben sich ***CyberCash Inc.***, ***Dresdner Bank AG*** und ***Sachsen LB***[51] zu einer Arbeitsgruppe zusammengefunden. Die Zusammenarbeit soll der Grundstein für eine Kooperation zwischen Banken, Kreditkartenprozessoren und Händlern in Deutschland sein. Die Partner beabsichtigen, dem deutschen Handel unter Verwendung international anerkannter Technologien die Abwicklung sicherer Point-of-Sale-Zahlungen im Internet anzubieten.

In einem ersten Schritt ist die Einführung des CyberCash-Kreditkarten-Service vorgesehen. Das System ermöglicht den im Internet präsenten Händlern und Dienstleistern zu jeder Tages- und Nachtzeit den Verkauf von Waren sowie die Abrechnung von online erbrachten Leistungen. In den USA wird dieser Service seit 1995 von CyberCash betrieben, wobei mehr als 300 Händler dem System angeschlossen sind. Obwohl sich CyberCash dem nach dem gegenwärtigen Stand der Technik effektivsten Verschlüsselungsverfahren RSA (1024 bit) und DES (56 bit) bedient, wird das Secure Electronic Transaction-Protokoll SET, ein von Visa und Mastercard gemeinsam initiiertes, kommendes Protokoll für Visa- und Mastercard-Zahlungen, nach seiner globalen Einführung automatisch für den sicheren Kreditkarten-Service übernommen.

Der CyberCoin-Service soll in einem zweiten Schritt angeboten werden. Dieser ist bereits seit Oktober 1996 in den USA eingeführt und ermöglicht die direkte Bezahlung von Nachrichten, Informationen, Software oder ähnliche Angebote, also Leistungen, die für die Bezahlung mit Kreditkarte nicht geeignet sind.

---

[51] http://www.sachsen-lb.de

11.4 Deutsche Banken im Internet (Auswahl)

Adig	http://www.adig.de
Advance Bank	http://www.advance-bank.de
Bank 24 Online-Banking	http://www.bank24.de
Bankgesellschaft Berlin	http://www.bankgesellschaft.de
Comdirect	http://www.comdirect.de
Commerzbank	http://www.commerzbank.de
Consors Diskount Broker	http://www.consors.de
Deutsche Bank Online-Banking	http://www.deutsche-bank.de
Dresdner Bank Online-Banking	http://www.dresdner-bank.de
Direkt Anlage Bank Online-Banking	http://www.diraba.de
DG-Bank Info-Service	http://www.dgbank.de
DIT Online-Banking, Info-Service	http://www.dit.de
DWS Info-Service	http://www.dws.de
Gries und Heissel Online-Banking	http://www.guh.de
HelabaTrust	http://www.helaba-trust.de
Landesgirokasse Stuttgart	http://www.lgbank.de
Quelle Bank	http://www.quelle.de
Sparda-Bank Hamburg Online-Banking	http://www.sparda-hh.de
Sparkassen im Netz	http://www.snet.de
Stadtsparkasse Dortmund Online-Banking	http://www.stadtsparkasse-dortmund.de
Union Investment	http://www.union-investment.de
Vereinsbank	http://www.vereinsbank.de
West LB	http://www.westlb.de
Frankfurter Sparkasse 1822	http://www.fraspa1822.de

12. Ausblick

Der Bereich „Electronic Commerce und Internet“ mit der Thematik des elektronischen Zahlungsverkehrs ist die bedeutendste interaktive Online-Transaktionsform, die gegenwärtig in Publikationen, Workshops und Foren diskutiert wird. Ursprünglich waren zunächst amerikanische Pionierfirmen wie Terisa Systems und Netscape die Wegbereiter, die mit Referenzimplementationen wie S-HTTP und SSL-Protokollen, zumindest für die Übermittlung von Kreditkarteninformationen, eine sichere Verschlüsselung anboten.

Nachdem die Bedeutung und Chancen der kommerziellen Nutzung des Internets auch den größeren Unternehmen der Informations- und Kommunikationsindustrie, den Banken und der Finanzwelt deutlich wurde, haben diese auf breiter Front Lösungsansätze für Protokollspezifikationen entwickelt und das Ringen um den dominierenden Standard eröffnet. IBM veröffentlichte 1995 einen Vorschlag namens iKP (Keyed Payment Schemes) zur Bezahlung mit Kreditkarten im Internet. Der Versuch dieses Protokoll, im Rahmen einer Zertifizierung durch die Internet Engineering Task Force Working Group (IETF-WG), als Standard durchzusetzten schlug aber fehl. Auch die Kreditkartengesellschaften drängten mit unterschiedlichen Lösungsansätzen für Protokollspezifikationen auf den Markt und sorgten zeitweise für Verwirrung. Microsoft und VISA kooperierten und entwickelten eine Spezifikation namens STT (Secure Transaction Technology). Daraufhin entwickelte ein Konsortium bestehend aus Mastercard, IBM, Netscape und CyberCash den Standard SEPP (Secure Electronic Payment Protokoll), der aus einer Zusammenfassung der verschiedenen Lösungsansätze von IBM (iKP), Netscape Secure Courier und CyberCash bestand. Zum Vorteil der Online-Nutzer einigten sich alle Beteiligte, vor allem Mastercard und Visa auf einen gemeinsamen Standard für sichere Kreditkartentransaktionen namens SET (Secure Electronic Transaktion), der noch in diesem Monat (Mitte April) abschließend begutachtet wird und in diesem Jahr zur offiziellen Markteinführung freigegeben werden soll.

Bis zum heutigen Zeitpunkt und voraussichtlich auch noch bis zur offiziellen Freigabe von SET wird aber noch weiterhin der SSL (Secure Socket Layer) von Netscape bzw. Terisa`s S-HTTP (Secure Hypertext Transport Protocol) zur Kreditkartenverschlüsselung benutzt. Die elektronische Shopping Mall „Intershop-Online[52]“, ein Prodokt des Unternehmens Intershop

---

[52] http://www.interschop.com

aus Jena, gilt weltweit als eine der fortschrittlichsten Malls im Bereich „Electronic Commerce und Electronic Shopping". Sie bietet für Kreditkartentransaktionen beide Protokolle an und verweist auch auf den zukünftigen Kreditkartenstandard SET. Darüber hinaus hat Intershop-Online auch eine Variante für den Bereich direkter Zahlungen kleinerer Beträge mit Hilfe der elektronischen Geldbörsen (Wallet) standardmäßig bereits implementiert.

Die im Rahmen dieses Projektkurses zentrale Frage einer möglichen Implementierung eines sicheren Bezahlsystems (z. B. im Rahmen der EMB) unter pragmatischen Gesichtspunkten, könnte durch ein Vorhaben der Dresdner Bank und der Sachsen LB in Kooperation mit CyberCash beantwortet werden. Im Gegensatz zum Internet-Banking, bei dem primär die Homebanking-Funktionalität auf das Internet übertragen wurde, entwickelte die Dresdner Bank, die Sachsen LB und CyberCash ein Internet-Bezahlsystem für Deutschland. Die Partner beabsichtigen dem deutschen Handel unter Verwendung international anerkannter Technologien die Abwicklung sicherer Point-of-Sale-Zahlungen im Internet anzubieten. Diese Dienstleistung sieht zwei Zahlungsvarianten vor, erstens die Kreditkartenzahlung und zweitens die direkte Zahlung mit Hilfe von CyberCoins über die elektronische Geldbörse. Die Software kommt von der Firma CyberCash. Konsumenten könnten beide Zahlungsarten unter Verwendung einer einheitlichen Software, dem CyberCash-Wallet benutzen. Für den Online-Händler bietet die Lösung von CyberCash, Dresdner Bank und Sachsen LB die Autorisierung und Abrechnung der im Internet erzielten Umsätze über die dem System angeschlossenen Banken. Darüber hinaus entwickelt CyberCash auch eine Zahlungsvariante mit der Funktionalität des „Elektronischen Schecks". Alle Zahlungsvarianten werden bei CyberCash als reine Softwarelösung implementiert. Hardwareerweiterungen wie z. B. der Me-Chip (Sparda Bank) oder die Smartcard-Konzeption (DigiCash) im Zahlungsverkehr von kleinen Beträgen (Tokenbereich) sind somit nicht mehr notwendig. Das Engagement der Dresdner Bank mit CyberCash und der Sachsen LB hat das Ziel einen Standard für Zahlungen im Internet zu schaffen und könnte für die EMB einen Lösungsweg für eine pragmatische Implementierung aufzeigen.

Kritische Anmerkung:

Angesichts der zu erwartenden Verbreitung des elektronischen Zahlungsverkehrs im Konsumentenbereich und der dadurch notwendigen Investitionen muß durch den Einsatz von adäquaten Sicherheitsmechanismen verhindert werden, daß das Vertrauen der Verbraucher in die Zuverlässigkeit und Korrektheit der Online-Systeme beeinträchtigt wird. Ebenfalls nicht vernachlässigt werden sollte der Datenschutz bei elektronischen Zahlungssystemen. Es muß für den Kunden nachvollziehbar sein, welche Stellen seine Daten zu welchen Zwecken weiterverarbeiten. Gegen den Willen des Kunden darf aufgrund seines Kaufverhaltens kein Kundenprofil erstellt werden, damit er beispielsweise bei seinem nächsten Einkauf nicht mit gezielter Werbung überschüttet werden kann. Sicherheit und Datenschutz sind die Grundlage für die Akzeptanz elektronischer Zahlungsverfahren im Internet.

13. Literaturverzeichnis

[ABI9449] Du Rea, M; Pemperton, J.M: „Electronic Mail and Electronic DataInterchange", Record Management Quarterly, Volume/Numer: 28 4 3-12, in ABI/INFORM, Issue: 9449, 1994.

[ABI9644] „Java Electronic Commerce Framework", Computer Reseller News, Volume/Number: 702 126-128, in ABI/INFORM, Issue: 9644, 1996.

[Bra96] Brauckmann, N.: „Kerberos schützt Host-Sessions: Sicherheit in Client/ServerUmgebungen", in LANline No.6, 196ff., 1996.

[Com96] Computerwoche 50/96, 13.

[Dra95] Dratva, R.: „Elektronische Informationsdienste: Zukunftweisende Konzepte und prototypische Umsetzung im Bankenbereich", S.95-126, in Schmid, B./Dratva, R./Kuhn, C./Mausberg, P./Meli, H./Zimmermann, H.D. Banking und Shopping in globalen Netzen, Stuttgart 1995.

[Egn96] Egner, T.: „EDIFACT im Zahlungsverkehr", in Congress IV, C424.01 in Online, Hrsg. J. Fischer, 1996..

[Fox95] Fox, D.: „Private Email, Schlüsseldienst - Private Kommunikation mit PEM und PGP", in C'T (Heise Verlag), Heft 9, S.184-187, 1995.

[Hüb96] Hübner, R.: „Der Chip auf dem Sprung", in Geldinstitute, No.10, S.50-52, 1996.

[Jan95] Janson, P., Waidner, M.: „Elektronic Payment over open networks", 1995.

[Jtk95] Jerman-Blazic, B./Trcek, D.: „A tool for support for key distribution and validity certificate in global Directory service", in Computer Networks and ISDN Systems,Vol.28, No.5.,709-717, 1996.

[Kal96] Kalakota, R./Whinston, A.B.: „Frontiers of Electronic Commerce" Addison Wesley 1.Aufl. 1996

[Kno96] Knoblauch, W.: „Vermarktung auf dem Internet: Chancen, Risiken und Technik“, in Congress IV, C434 in Online 1996, Hrsg. J. Fischer und IBM Europäisches Zentrum Heidelberg 1995.

[Kon93] Kohl, J./Neumann, C.: „The Kerberos Network Authentification Service“, Massachusetts Institute of Technology, 1993.

[Kuhlen 96] Rainer Kuhlen: Electronic Mall Bodensee - ein grenzüberschreitender elektronischer Marktplatz, in Thomas Ellwein, Lürgen Mitelstraß (Hg.), Region-Regionalismus-Regionalentwicklung, Isensee Verlag, Oldenburg, 1996.

[Mau95] Mausberg, P.: „Die Elektronische Abwicklung des ZV privater Kunden auf der Basis eines standardisierten Nachrichtenaustausches“ , S. 181ff., in Schmid, B./Dratva, R./Kuhn, C./Mausberg, P./Meli, H./Zimmermann, H.D. Banking und Shopping in globalen Netzen, Stuttgart 1995.

[Mes95] Messmer, E.: „NASA launches Internet EDI purchasing program“, in Network World, Volume / Number 12,7 1995 in ABI/INFORM Issue 9510, 1995.

[Mit96] Mitchell, R.: „Marking the Connection“, Credit Card Management, Volume / Numer 9, 105-106 in ABI/INFORM Issue 9651, 1996.

[Mu95] Muiznieks, V.: „The Internet and EDI“, in ABI/INFORM Issue 9549, Journal Telecommunications Volume/Number 29, 11, 45-48, 1995.

[Neu96] Neuburger, R., „EDI und Internet: Können sie sich sinnvoll ergänzen“, in Congress IV, C426 in Online 1996, Hrsg. J. Fischer.

[Pfeffer96] Pfeffer, Christine.: Authentifizierung und Zertifizierung im elektronischen Zahlungsverkehr, Diplomarbeit am Lehrstuhl Informationswissenschaft, Universität Konstanz, 1996.

[Plat93] Plattner, B. et. al: „Elektronische Post und Datenkommunikation - x.400: Die Normen und ihre Anwendung“, Bonn. Addison Wesley, 3. Aufl. 1993.

[Pey96] Peyle, R.: „Electronic Commerce and the Internet“, in ACM Communication 39 6, S.23, 1996.

[PTS9539] Edge, Volume 10, Issue 374 „E-Banking: FSTC Unveils Electronic Check Technology - Secure, Versatile Instrument for Electronic Commerce“, in PTS Newsletters, Issue 9539, 1995.

[PTS9540] Multimedia Daily, Volume 2, Issue 184 „Electronic Check Unveiled“, in PTS Newsletter, Issue 9540, 1995.

[PTS9637] Brokat: „Technological breakthrough for secure banking & shopping over the Internet through X-Presso“in PTS Newsletters, Issue 9637, 1996.

[Reif95] Reif, H.: „Netz ohne Angst: Sicherheitsrisiko des Internets“, in c`t (Heise Verlag), Heft 9, S.174f., 1995.

[Sch96] Schneider, Bruce: „Applied Cryptography, Protocols, Algorithms and Source Code in C“, 2nd Edition, John Wiley&Sons, New York 1996.

[Schmidt et al. 95] B. Schmidt u. a.: Electronic Mall: Banking und Schopping in globalen Netzen. B. G. Teubner. Stuttgart 1995.

[Set96] SET Specifikation Internet Draft.

[Smo95] Carl-Mitchell, Smoot (1995), "The new Internet Protocol" in UNIX Review, Vol. 13, 7 S.31-38 in ABI/INFORM Issue 9524, 1995.

[Spi96] Spiegel Nachrichtenmagagzin, Ausgabe Nr.12/18.3.1996, 132.

[Str96] Ströbele, E.: „Pilotprojekt Geldkarte“, in Geldinstitute, No.10. S.54f, 1996.

[VDI96] VDI-Nachrichten Nr. 42, 11.10.1996, S.6.

[Zi95] Zimmermann, P.: „The official PGP User`s Guide“, in MIT Press Cambridge, 1995.

[Zim95] Zimmermann, H.D./Kuhn, C.: „Grundlegende Konzepte einer Electronic Mall“, S.33-89, in Schmid, B./Dratva, R./Kuhn, C./Mausberg, /Meli,H./Zimmermann, H.D.Banking und Shopping in globalen Netzen, Stuttgart 1995.