"Survival Skript"

Zur Vorlesung:

Einführung in die Wirtschaftsinformatik WS00/01 (bei Prof. Dr. J. Ruhland)

-Teil 5-

Hinweis: Dieses Skript wurde privat erstellt, um für die Wirtschaftsinformatik-Klausur eine Basis zu haben, und wird anderen Studierenden zur *privaten* Vorbereitung auf die Klausur ebenfalls zur Verfügung gestellt. Eine - wie auch immer geartete - kommerzielle Nutzung des "Survival-Skriptes" stellt einen Verstoß gegen die Urheberrechte der div. benützten (und nicht immer explizit ausgewiesenen) Quellen dar. Als "Privat-Papier" kann auch keine Garantie auf Vollständigkeit und/oder Fehlerfreiheit gegeben werden. Man sollte aber ruhig davon ausgehen, das dieses Skript hier als Lerngrundlage einigermaßen zuverlässig ist. Fragen und / oder Anregungen bitte an: bast4u@gmx.net

Inhaltsverzeichnis

5. Anwendungssysteme in Auswahl 2

5.0 Hinweis zum Skript 2

5.1 Warenwirtschaftssysteme - Stichwort EAN & Co 2

5.1.1 Identifikationssysteme für automatische Datenerfassung 2

5.1.1.1 Das System der internationalen Lokationsnummerierung (ILN) 2

5.1.1.2 Die ILN: Zugriffsschlüssel auf Datenbankinformationen 3

5.1.1.3 Die Anwendungen der ILN 3

5.1.2 Die Internationale Artikelnummer (EAN) 4

5.1.2.1 Aufbau der EAN 4

5.1.2.2 Anwendungen der EAN 6

5.2 eCommerce 7

5.2.1 Was ist Electronic Commerce? 7

5.2.2 Ist Electronic Commerce sicher für den Anbieter? 7

5.2.3 Ist Electronic Commerce sicher für den Kunden? 7

5.2.4 Gibt es technologische Standards für Electronic Commerce? 8

5.2.5 Welche Schlagwörter muss man kennen? 8

5.2.6 Was kann online gekauft werden? 9

5.3 Homebanking, Sicherheit und eCash 10

5.3.1 Schlagworte zu Homebanking & Sicherheit 10

5.3.2 Sichere Übertragung im Internet: SSL 11

5.3.3 eCash: Auszüge aus einem Vortrag zum Thema eCash 16

5.3.3.1 Einleitung 16

5.3.3.2 Signaturen 16

5.3.3.3. Electronic Cash 18

5. Anwendungssysteme in Auswahl

5.0 Hinweis zum Skript

Das Kapitel 5 - Skript ist nicht mehr so aussführlich 8oder eigentlich garnicht) ausformuliert wie die anderen. Das hat zwei Gründe: Zum einen habe ich einfach keine Zeit mehr, und zum anderen sind meiner Meinung nach die jew. Punkte *entweder* im "Ruhland-Skript" gut nachvollziehbar, *oder* ich habe sehr lesbare "fremd"Texte gefunden.

5.1 Warenwirtschaftssysteme - Stichwort EAN & Co

Hier habe ich einfach den "Werbetext" einer Webside abgedruckt, ich denke da wird dann (zusammen mit dem Ruhland Skript) schon klar welcher Gedanke dahinter steckt.

Quelle: Centrale für Coorganisation (http://www.service.ccg.de/)

5.1.1 Identifikationssysteme für automatische Datenerfassung

Im Bereich "Identifikationssysteme" geht es um die Entwicklung,
Pflege und Einführung der EAN-Nummern- und -Codiersysteme. Dies sind
Internationale Lokationsnummer (ILN)
Internationale Artikelnummer (EAN)
~~Nummer der Versandeinheit (NVE)~~
jeweils mit ergänzenden Codierungen und Strichcodes.

5.1.1.1 Das System der internationalen Lokationsnummerierung (ILN)Fehler! Textmarke nicht definiert.

Die Internationale Lokationsnummerierung (ILN) stellt eine Grundvoraussetzung des rationellen zwischenbetrieblichen Informationsaustausches dar. Die ILN wird benötigt, um Güter, papiergebundene Informationen oder elektronische Daten an den gewünschten Ort die richtige Adresse zu liefern.

Mit Hilfe der ILN können physische Adressen von Unternehmen, Tochterunternehmen, Niederlassungen und sogar Regionalbüros eines Unternehmens identifiziert werden. Eine ILN vermag darüber hinaus aber auch ablauforientierte Einheiten eines Unternehmens - wie Läger, Abteilungen, Produktionsstraßen, Lieferpunkte sowie Netzwerk- und sonstige Kommunikationsknoten - eindeutig zu identifizieren. Dabei wird die Nummer in allen Anwendungen als Zugriffsschlüssel auf die im Computersystem abgelegten Stammdaten verwendet.

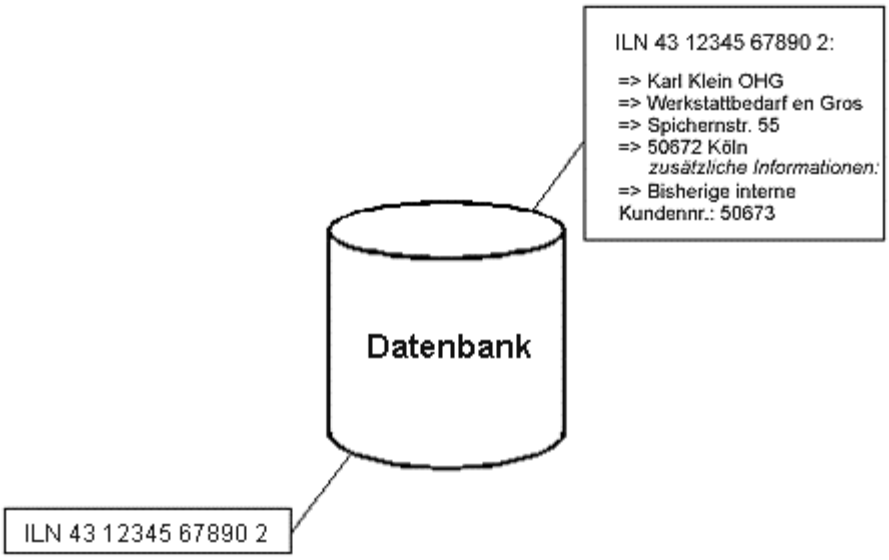
Die weltweit überschneidungsfreie Internationale Lokationsnummer ersetzt an den Kommunikationsschnittstellen von Industrie, Handel und Dienstleistungssektor die bis dato übliche Pflege bilateral abzustimmender Kunden- und Lieferantennummern. Sie hilft den Verwaltungsaufwand zu verringern, die Datenverarbeitungsprozesse zu vereinfachen sowie die Genauigkeit und Geschwindigkeit der Administrations- und Datenverarbeitungsprozesse zu erhöhen. Sie schafft zugleich die nötigen Voraussetzungen für ein effizientes Versenden, Sortieren und Verfolgen von Gütern und das Rückführen von Mehrweg-

Transportverpackungen.

Der Rückgriff auf die ILN stellt in den verschiedenen Kommunikationsverfahren sicher, daß es beim unternehmensübergreifenden Datenaustausch nicht zu Nummernüberschneidungen durch Kollision interner Systeme kommt. Die ILN ist keine "sprechende" Nummer, dadurch ist sie für jeden Anwender gleich gut im Sinne eines Schnittstellenidents zu verwenden.

In Deutschland identifizieren sich im Elektronischen Geschäftsverkehr (EDI) Ende 1997 84.000 Unternehmen und Betriebe mittels der ILN.

5.1.1.2 Die ILN: Zugriffsschlüssel auf Datenbankinformationen



5.1.1.3 Die Anwendungen der ILN

Die ILN im Formularwesen

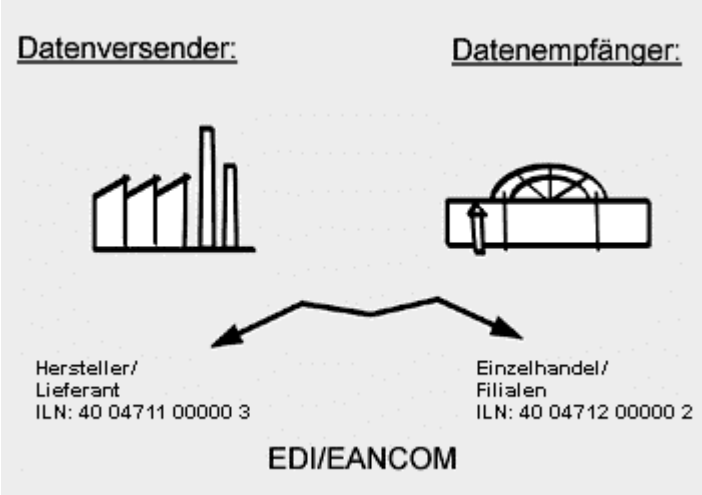
Im Formularwesen tritt die ILN an die Stelle von maschinell kaum zu erfassenden und EDV-technisch schwer zu verarbeitenden Adreßdaten. Als rein numerische Identifikation dient sie als Zugriffsschlüssel auf in Karteien oder Dateien abgelegte ausführliche Adreßinformationen. Platzersparnis auf dem Formular sowie Fehlerreduzierung und Zeitersparnis bei der Verarbeitung von Adressen sind die Folge.

Die ILN im elektronischen Datenaustausch

Im Rahmen des elektronischen Datenaustausches müssen Lokationsstammdaten durch die Verwendung der ILN nicht für jeden einzelnen Geschäftsvorgang neu ausgetauscht werden. Die notwendigen Informationen werden allen Kommunikationspartnern einmal mitgeteilt, hinter der ILN in den Stammdateien abgelegt und für die unterschiedlichen Datenverarbeitungsprozesse mit Hilfe dieses Schlüssels wieder abgerufen. Als Konsequenz ergeben sich Rationalisierungspotentiale wie

- Reduzierung der Übertragungskosten
- weniger Speicherplatz
- vollautomatische Datenverarbeitung
- sichere Datenverarbeitung
- korrektes Routing von elektronischen Nachrichten

- in die jeweilige Mailbox, Workstation oder Anwendung



ILN im Strichcode

In logistischen Anwendungsumgebungen kann die ILN zum Zwecke der schnellen und fehlerfreien Erfassung in strichcodierter Form wiedergegeben werden. Zum Beispiel ist die Darstellung der ILN des Warenempfängers als Routinginformation sowie die Wiedergabe der ILN des Warenversenders und Rechnungsempfängers im Strichcode EAN 128 vorgesehen.

5.1.2 Die Internationale Artikelnummer (EAN)

Reibungsloser Austausch von Geschäftsdaten sowie der rationelle Einsatz automatischer Lese- und Steuerungssysteme erfordern

überschneidungsfreie Identnummern schnittstellen übergreifende, maschinenlesbare Codierungen

Das System der Internationalen Artikelnummerierung EAN schafft die hierfür notwendige Voraussetzung.

5.1.2.1 Aufbau der EAN

Jede EAN-Artikelnummer geht aus von der sog. Basisnummer, die in Deutschland von der CCG im Zusammenhang mit einer ILN-Lokationsnummer (vom Typ 2) auf Antrag vergeben wird. Die EAN-Artikelnummer ist im Normalfall 13stellig und rein numerisch. Sie wird vom Hersteller/Vertreiber/Importeur des Artikels selbständig und in Eigenverantwortung auf Basis der ihm von der CCG zugeteilten ILN (Typ 2) vergeben.

Die EAN-13 hat folgenden Aufbau:

Internationale Artikelnummer (EAN-13)		
Basisnummer	individuelle Artikelnummer	Prüfziffer
40 1 2 3 4 5	1 2 3 4 5	6
z.B. Leguan Schulfüller "de Luxe"		

Vorgehensweise zur Bildung einer EAN:

Im Anschluß an die sieben Stellen der Basisnummer erfolgt Vergabe von fünf weiteren Ziffern nach eigener Wahl für jeden Artikel Ermittlung der Prüfziffer (13. Stelle) nach dem EAN- Prüfziffernalgorithmus

EAN-Kurznummer

Für besonders kleinvolumige Artikeln, bei denen eine Auszeichnung mit EAN-13 aus Platzgründen nicht möglich ist (z.B. Streichholzschachteln, Radiergummis), können 8stellige Kurznummern verwendet werden. Diese Identnummern können, wenn die Notwendigkeit ihrer Anwendung nachgewiesen werden kann, bei der CCG einzeln beantragt werden. Sie werden nicht mittels einer Basisnummer gebildet, sondern werden direkt und komplett von der CCG aus einem dafür reservierten Nummernkreis vergeben.

Besondere Bereiche

Für einige Branchen und Wirtschaftsbereiche empfiehlt die CCG Sonderformen der Identifikation.

Handelsinterne Ergänzungsnumerierungen

Auch Handelsunternehmen müssen die Möglichkeit haben, ergänzend zum sog. Source Marking - ohne die Industrie - eigene Artikelnummern zu bilden und gegebenenfalls zu codieren. Dies gilt insbesondere dann, wenn Waren gekennzeichnet werden müssen, die seitens der Hersteller/Importeure nicht ausgezeichnet sind. Für solche handelsinternen ("In-store") EAN, die wegen fehlender Überschneidungsfreiheit nicht betriebsübergreifend eingesetzt werden können, sind im EAN-System die Präfixe "2" bzw. "20" reserviert.

Codierung gewichts-/mengenvariabler Artikel

Für nicht egalisierte, also gewichts- oder mengenvariabel abgepackte Ware, bei der jede Packung auch einen anderen Preis hat (z.B. Käse, Wurst, Obst), sieht das EAN-System in Deutschland eine Spezialcodierung im Rahmen der handelsinternen Ergänzungen mit den Vorziffern 21 bis 29 vor.

Einzelheiten siehe die einschlägigen Veröffentlichungen. Dadurch wird die Möglichkeit geschaffen, daß die Scannerkasse den Preis oder das Gewicht/Stückzahl direkt dem Strichcode auf dem Etikett entnimmt.

Gesteuert wird dieses System durch die Anwendung verschiedener Systemkennzeichen.

Codierung von Büchern, Zeitungen und Zeitschriften

Das EAN-System läßt für Bücher und Zeitschriften die Integration von ISBN (International Standard Book Number mit Systemkennzeichen 978) bzw. ISSN (International Standard Serial Number mit Systemkennzeichen 977) in die EAN-13 zu.

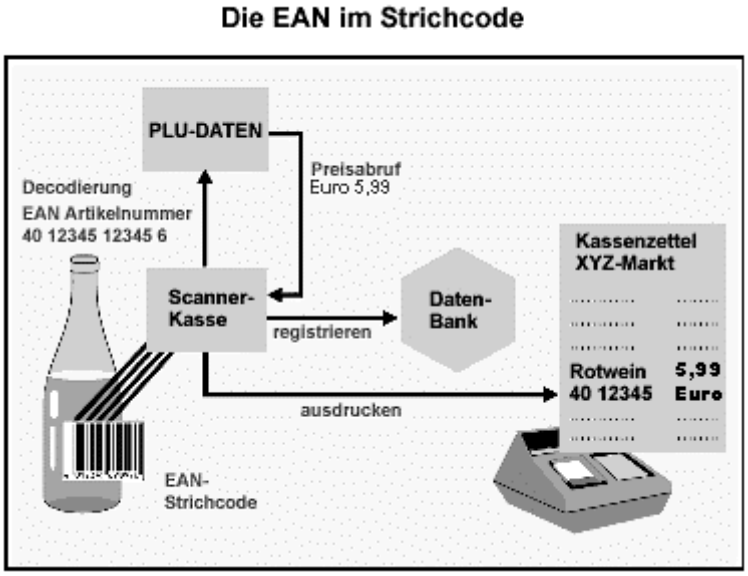
In Deutschland ist für Zeitungen und Zeitschriften ein EAN-Code zulässig, der zum einen eine von der CCG vergebene Objektnummer integriert und zum anderen den ladengebundenen Verkaufspreis (unmittelbare Preisbindung) enthält. Auf diesem Wege können die Retouren beim Presse-Grosso besser gesteuert werden. Zur Kennzeichnung der beiden verschiedenen, in der Pressebranche üblichen Mehrwertsteuersätze werden die Systemkennzeichen "439" (bei Titeln mit ermäßigtem Mehrwertsteuersatz) und "434" (bei Titeln mit vollem Mehrwertsteuersatz) verwendet.

Nutzen Sie bitte die Möglichkeit der Online-Bestellung entsprechender CCG-Publikationen.

5.1.2.2 Anwendungen der EAN

Die EAN im Strichcode

Die strichcodierte Umsetzung der EAN-Nummer in eine maschinenlesbare Schrift ermöglicht ihre automatisierte Verarbeitung im Umfeld verschiedenster Anwendungen wie



- Scanning an Datenkassen im SB-Groß- und Einzelhandel (Preisabrufverfahren "PLU")

- Inventur
- Wareneingang
- Kommissionierung
- Produktionssteuerung ....

Neben dem Einbeziehen in den Verpackungsmitteldruck besteht eine Vielfalt von Möglichkeiten, die EAN-Artikelnummern auch nachträglich (z.B. per Etikett) strichcodiert darzustellen und auf Packmittel aufzubringen. Ein EAN-Symbol setzt sich zusammen aus dunklen Strichen auf hellem Hintergrund. Bei der Auswahl der Balken- bzw. Hintergrundfarbe ist immer zu beachten, dass die entsprechenden Kontrastwerte für den Scanner hoch genug sind. Ebenfalls ist die richtige Strichcode-Schriftgröße in Abhängigkeit vom Druckverfahren auszuwählen (Mindestgröße: Breite 30,50 mm x Höhe 21,48 mm beim EAN-13).

Die EAN in der Warenwirtschaft

Die EAN ist einer der wichtigsten Bausteine moderner Warenwirtschaftssysteme. So ist sie z.B. beim Scanning im Handel Grundlage der Verkaufsdatenerfassung und Schlüssel bei der Weiterverarbeitung der Daten in den internen Organisationsstrukturen des jeweiligen Unternehmens.

Die EAN im Formularwesen

In den Bestell-, Abrechnungs- und Lieferpapieren ersetzt die EAN die individuellen Artikelnummern von Herstellern, Lieferanten und Kunden. Aufwendiges manuelles Umcodieren ist nicht erforderlich.

Die EAN im Elektronischen Datenaustausch (EDI)

So wie die ILN den Sender und Empfänger einer Nachricht identifiziert, kennzeichnet die EAN im elektronischen Geschäftsverkehr den Artikel, über den kommuniziert wird.

5.2 eCommerce

"(Zitat)

5.2.1 Was ist Electronic Commerce?

Viele Menschen setzen Electronic Commerce mit dem deutschen Begriff "Elektronischer Handel" gleich. Oft denken sie dabei in erster Linie an die neuen Einkaufsmöglichkeiten: Online können elektronisches Spielzeug, Bücher oder CDs bestellt werden. Aber Electronic Commerce bedeutet wesentlich mehr. Dazu gehört der gesamte Geschäftsprozeß, von Werbung, Geschäftsanbahnung und -abwicklung bis hin zu After-Sales Services, Aktionen zur Kundenbindung und Online Banking im neuen elektronischen Medium. Im weitesten Sinne fällt darunter z.B. auch der Handel mit CD-Rom-Unterstützung oder Faxabruf. Electronic Commerce findet also nicht nur im Verhältnis Anbieter und Konsumenten (Business-to-Consumer) statt. Wesentliche andere Einsatzfelder sind der elektronische Geschäftsverkehr zwischen Unternehmen (Business-to-Business), zwischen Konsumenten und öffentlichen Einrichtungen (Consumer-to-Administration), oder zwischen Unternehmen und öffentlichen Einrichtungen (Business-to-Administration). Ist Electronic Commerce also im Grunde lediglich die Fortsetzung des Geschäfts mit elektronischen Mitteln? Wahrscheinlich nicht, denn in der letzten Zeit geht ein wesentlicher Trend immer stärker in eine Richtung, die auf den ersten Blick eigentlich gar nichts mehr mit Kommerz zu tun hat: die Bildung virtueller Gemeinschaften, sogenannter Communities. Die neuen Kommunikationsmöglichkeiten werden von den Internetnutzern schon seit ihrer Entstehung rege mit Leben gefüllt. Mittlerweile haben auch Unternehmen erkannt, dass sich gerade in diesen Bereichen völlig neue Geschäftschancen entwickeln. Menschen mit gleichen Interessen treffen sich nunmehr auch zum privaten und geschäftlichen Austausch im Rahmen von Angeboten, die kommerziell betrieben, von Unternehmen gesponsert oder beworben werden. Eins ist klar: Electronic Commerce ist vielfältig. Das neue Medium bietet ein Spektrum von Möglichkeiten, aber die Unternehmen müssen sie betriebswirtschaftlich sinnvoll und kreativ nutzen. Nur Mut, Rom wurde auch nicht an einem Tag erbaut!

5.2.2 Ist Electronic Commerce sicher für den Anbieter?

Vorausgeschickt: Absolute Sicherheit gibt es in keinem Bereich, auch nicht im traditionellen Geschäft. Aber schafft Electronic Commerce vielleicht weitere, zudem leicht zugängliche Angriffspunkte? Schließlich ist leicht einzusehen, dass Server, auf denen sensible Daten abgespeichert werden, ein besonders attraktives Ziel sind. Messungen haben ergeben, dass Angriffe auf Server mit Electronic Commerce Angeboten wesentlich öfter vorkommen als auf andere Sites. Bisher sind jedoch kaum erfolgreiche Angriffe bekannt geworden. Das mag einerseits damit zusammenhängen, dass Betroffene natürlich wenig Interesse am Bekanntwerden einer solchen Panne haben. Andererseits werden die Systeme aufgrund der immer weiter verbreiteten Sensibilisierung der Betreiber immer sicherer. Es gibt inzwischen etliche Hilfsmittel, mit denen sich ein Webserver auf seine Sicherheit gegen Angriffe von außen testen lässt. Beispielhaft sei hier SATAN ("Security Analysis Tool for Auditing Networks") genannt, das trotz seines Namens eine sehr gute Analyse-Software ist und durch simulierte Angriffe Schwachstellen findet. Fazit: Sichere Architektur ist machbar. Es ist ist nahezu unmöglich, in ein sauber administriertes UNIX-System einzudringen. Electronic Commerce stellt daher kein unkalkulierbares Risiko dar.

5.2.3 Ist Electronic Commerce sicher für den Kunden?

Viele Internetnutzer sind immer noch misstrauisch gegenüber Online-Transaktionen. Unsicherheiten bei der Zahlung über das Internet und Ängste vor möglicherweise hinterlassenen Datenspuren stehen bei den Kunden im Vordergrund. Trotz dieser Vorbehalte wachsen die Umsätze über das Internet weiterhin rasant.

Die Gefahr des Missbrauchs gestohlener Kreditkartendaten im Netz ist relativ gering. Online-Bestellungen entsprechen häufig den traditionellen Mailorder-Geschäften. Da dem Händler bei der Bestellung keine handschriftliche Unterschrift des Kunden vorliegt, trägt der Händler auch das Risiko etwaiger Falschbestellungen. Der Kunde kann bei der Lieferung von nicht bestellten Gütern die Zahlung verweigern. Die Kosten trägt dann der Händler. Von Fachleuten wird argumentiert, dass die Online-Übermittlung von Kreditkartennummern (die häufigste Art der Transaktion im Netz) wesentlich sicherer ist als die Zahlung

mit Karte im Restaurant. Es ist wesentlich leichter, einen achtlos weggeworfenen Beleg mit allen Daten aus einem Papierkorb zu fischen, als die Nummer technisch sehr aufwendig aus den Myriaden von Datenpaketen aus dem Internet herauszufiltern.

Schließlich gibt es inzwischen eine Reihe von Sicherheitsfeatures wie z.B. die Verschlüsselung der übertragenen Daten mit Secure Sockets Layer (SSL), die vom Netscape Navigator und vom MS Internet Explorer schon seit Version 2.0 unterstützt wird. Zu erkennen ist SSL daran, dass die Adresse mit "https://" (anstelle von "http://") beginnt bzw. dass beim Netscape Browser links unten der kleine Schlüssel intakt bzw. das Vorhängeschloß geschlossen ist.

Während viele gute Verfahren zum Schutz vor Diebstahl entwickelt werden oder bereits ausgereift sind, schenkt man dem Schutz privater Daten oft noch wenig Aufmerksamkeit. Aber auch darüber sollten Anbieter und Kunden nachdenken: Vertrauen ist gut, Transparenz ist besser!

5.2.4 Gibt es technologische Standards für Electronic Commerce?

Die Entwicklung von neuen technischen Lösungen für Electronic Commerce erfolgt in einem rasanten Tempo. Zusätzlich zu den allgemeinen Standards und Protokollen für das Internet oder auch andere Arten von Netzwerken gibt es zahlreiche bereits im Einsatz befindliche oder geplante Standards für Electronic Commerce. Bei den bereits erprobten handelt es sich häufig um Business-to-Business Übertragungsprotokolle, die z.B. an Electronic Data Interchange (EDI-) Formate anknüpfen

OBI (Open Buying on the Internet) soll die Kommunikation der unterschiedlichen Electronic Commerce Systeme möglich machen. Die erste Version wurde im Juni 1997 vom OBI Konsortium veröffentlicht und wird von wichtigen Unternehmen wie z. B. Microsoft, Open Market und Oracle unterstützt. Im August 1999 wurde die Version OBI V2.0 Standard vorgestellt.

SET (Secure Electronic Transactions) sorgt als Industriestandard bei Zahlungen per Kreditkarte über das Internet mit Hilfe von Zertifikaten, die die Identität der Parteien der Transaktion bestätigen, für Sicherheit. SET wurde von VISA und Mastercard entworfen und stellt die Grundlage für unterschiedliche Transaktions-Software dar. Mehr zu SET finden Sie in unseren Rubriken Zahlungssysteme und Sicherheit.

SSL (Secure Socket Layer) stellt sichere Verbindungen zu einem WWW-Server her. Es arbeitet mit Public-Key-Verschlüsselung, um die übertragenen Daten zu schützen. Entwickelt wurde das Protokoll von Netscape, ist allerdings nun allgemein zur Benutzung freigegeben. Mehr zu SSL finden Sie in unserer Rubrik Sicherheitoben

XML (Extensible Markup Language) ist eine Seitenbeschreibungssprache, die über HTML hinausgehende Möglichkeiten bietet. In dieser vereinfachten Version der Standard Generalized Markup Language (SGML) können eigene Dokumenttypen, die die Bedeutung des Inhalts beschreiben, festgelegt und so über Plattformgrenzen hinweg ausgetauscht werden. Vor allen Dingen im B2B-Bereich wird eine problemlose Datenkommunikation möglich. Mehr zu XML finden Sie in unserer Rubrik EDI & EC.

HBCI (Home Banking Computer Interface), ist ein Standard für die sichere Abwicklung von Online-Bankgeschäften. Durch asymmetrische Verschlüsselungsverfahren und digitale Signaturen wird die Verwendung von Persönlichen Identifikationsnummern (PIN) und Transaktionsnummern (TAN) überflüssig. Mehr zu HBCI fnden Sie in unserer Rubrik Zahlungssysteme.

5.2.5 Welche Schlagwörter muss man kennen?

Electronic Commerce ist voll von oft englischen Schlagwörtern. Die Wichtigsten haben wir hier für Sie zusammengestellt: Digital oder Electronic Cash (auch e-cash oder e-money genannt): alle elektronischen Verfahren, mittels derer man Waren und Dienstleistungen durch Übertragung elektronischer Datenpakete von einem Computer zum anderen "bezahlen" kann. Diese Pakete sind jeweils einmalig und funktionieren genau wie die Seriennummern auf einem Geldschein. Sie werden durch eine Bank herausgegeben und stellen eine bestimmte Geldsumme dar. Eine der Haupteigenschaften von Electronic

Cash ist, dass es anonym und mehrfach verwendbar ist, genau so wie normales Geld. Dies ist der wichtigste Unterschied zwischen e-cash und Kreditkartenabwicklung über das Internet. Eine ausgereifte Umsetzung ist z.B. ecash von der Firma Digicash.

Disintermediation
Ausschalten des Zwischenhändlers. Webbasierte Firmen umgehen traditionelle Einzelhandelskanäle und verkaufen direkt an den Kunden. Traditionelle Intermediäre wie z.B. Einzelhandelsläden und Warenversandhäuser könnten durch die neuen Möglichkeiten des Direktverkaufs über das Internet ernsthaft gefährdet werden.

Electronic Payment Systems (elektronische Zahlungssysteme)
Sammelbegriff für alle verschiedenen elektronische Zahlungsformen im Internet. Mehr dazu finden Sie in unserer Rubrik "Elektronische Zahlungssysteme".

Extranet
Ein Netzwerk zwischen verschiedenen geographischen Punkten (z.B. zwischen verschiedenen Niederlassungen einer Firma oder Firmen und Kunden/Lieferanten), basierend auf Internet-Technologie. Dadurch wird die Entstehung von e-Commerce Anwendungen ermöglicht, welche alle Aspekte einer geschäftlichen Beziehung verbinden, angefangen beim Einkauf bis hin zur Zahlung, ohne über das öffentliche Internet zu gehen.

Intranet
Ein Netzwerk innerhalb eines Gebäudes, das auf Internet-Technologie basiert. In den letzten Jahren wurden immer mehr Inhaus-Netze von proprietären Technologien auf TCP/IP umgestellt, da es sich laut weit verbreiteter Meinung a) um eine bewährte, betriebssystem-unabhängige Technologie handelt und b) gut mit externen Netzen verbinden lässt.

Micro Payment
Zahlungssysteme für Kleinstbeträge zwischen 25 Cent und 10 Dollar wie z. B. Millicent von der Firma Digital. Sie eignen sich insbesondere für Einmalzahlungen für kleine Programme, Grafiken, Spiele und Informationen (z.B. Seiten mit Aktienkursen oder Fachbeiträge). Pay-as-you-go Mikrozahlungen sollten die E-Commerce-Welt revolutionieren. Da es die meisten Informationen jedoch noch kostenlos an anderer Stelle im Netz zu finden gibt, sind die meisten nicht bereit, für Leistungen zu bezahlen.

Wallet (Geldbörse)
Eine Software wie z. B. das Internet Wallet von CyberCash, das Ihre Kreditkartennummer verschlüsselt auf Ihrer Festplatte speichert. Sie können dann Online-Einkäufe bei den Webservern tätigen, die die von Ihnen benutzte Wallet-Software unterstützen. Wenn Sie einen beteiligten Online-Store besuchen, betätigen Sie einen Zahlungsbutton, um eine Kreditkartenzahlung durch eine gesicherte Transaktion auszulösen, welche durch den Server der Firma des "Electronic Wallet" aktiviert wird. Die wichtigsten WWW-Browser-Hersteller haben vertraglich abgesichert, dass sie die Technologie zur Unterstützung dieser Wallets in die Browser einbauen können.

5.2.6 Was kann online gekauft werden?

Nahezu jeder Einkaufswunsch lässt sich online nicht nur in den USA, sondern auch in Europa und in Deutschland erfüllen: Neben Computern und Software sind Lebensmittel, Bekleidung, Blumen, Wein und vieles andere mehr erhältlich. Ein großes Problem ist es jedoch noch immer, die gewünschten Produkte schnell und bequem zu finden.

Als großer deutscher Anbieter präsentiert z.B. Karstadt ein umfassendes Warenhaussortiment, ebenso wie die Versandhandelsunternehmen Otto, Quelle und Neckermann. Nach durchgreifenden Neugestaltungen in den letzten Jahren offerieren viele Versandhändler mittlerweile fast ihre gesamte Produktpalette einschließlich von Sonderangeboten online. Aber auch

speziell auf die Online-Kundschaft zugeschnittene Angebote sind keine Seltenheit mehr. So bedient Otto die jüngere Clientel mit der P.S. Company.

Im Business-to-Business sind insbesondere in der letzten Zeit zahlreiche deutsche Unternehmen aktiv geworden. Eine Anfang 2000 erschienene Studie von Forrester belegt, dass drei Viertel der Lieferanten und fast die Hälfte der Einkäufer Formen des E-Commerce in ihren Transaktionen anwenden. Dementsprechend wächst die Zahl der B2B-Marktplätze oder ‚Vortals' (Vertikale Portale) rasant. International sehen die Experten der Delphi Group jedenfalls den Erfolg der elektronischen Marktplätze für Business-to-Business Transaktionen schon jetzt: über Vortals sollen im Jahr 2002 Umsätze in Höhe von 5 Billionen US$ abgewickelt werden. Nach ihrer Einschätzung belegt die positive Entwicklung von Unternehmen wie Free Markets, VerticalNet oder Ariba die stark wachsende Bedeutung der Koordinierung von Angebot und Nachfrage durch branchen- und industriespezifische Plattformen. Die Aufmerksamkeit von Kapitalgebern haben die Vortals schon gewonnen, so stellen z.B. EDS und AT Kearney Ventures 1,5 Mrd. US$ für Vortal-Unternehmen zur Verfügung und CMGI hat bereits in Chemdex und SilkNet investiert.

In der Konsequenz ist die Palette der im Internet verfügbaren Waren und Dienstleistungen nahezu unbegrenzt: Die Frankfurter Metallgesellschaft AG z.B. bringt über das Tochterunternehmen mg electronic commerce service GmbH die Chemiebranche online. Bei Cheop, für ‚chemical opportunities' , werden Produkte wie Salzsäure und anderes online gehandelt, Preise verglichen und Informationen ausgetauscht. Aber auch die Energieversorger handeln Strom auf virtuellen Marktplätzen und Stromabnehmer können Anbieter frei wählen. An private Stromkunden wendet sich Strominfos.de. Ein Tarifrechner mit Datenbank ermöglicht Preisvergleiche zwischen den verschiedenen Anbietern

Neue Geschäftsmodelle machen darüber hinaus neue Produkte möglich. Procter & Gamble steigt zum Beispiel mit einer neuen Internet Company in den direkten Absatz ein. Reflect.com soll dabei wird den traditionellen Marken des Kosmetikkonzerns keine Konkurrenz machen. Explizites Ziel ist es vielmehr, die Produkte jeweils individuell an die Wünsche und Besonderheiten der einzelnen Kunden anzupassen. Customization und Service stehen im Mittelpunkt der radikal auf die Optionen des Internet konzentrierten Strategie. (Zitat Ende)" (Quelle: http://www.electronic-commerce.org/)

5.3 Homebanking, Sicherheit und eCash

5.3.1 Schlagworte zu Homebanking & Sicherheit

Homebanking

Zugriff vom eigenen PC auf Rechner oder Großrechner eines Geldinstitutes.
Geldtransaktionen/Bankgeschäfte von zu Hause aus innerhalb eines digitalen Mediums.
Online-Dienst = Online Banking, Internet = Internetbanking

Online - Banking

Im Gegensatz zum Internet besitzt ein Online – Dienst ein eigenes Datennetz und eigene Inhalte. Zugreifen können darauf nur Mitglieder des jeweiligen Anbieters.

Internetbanking

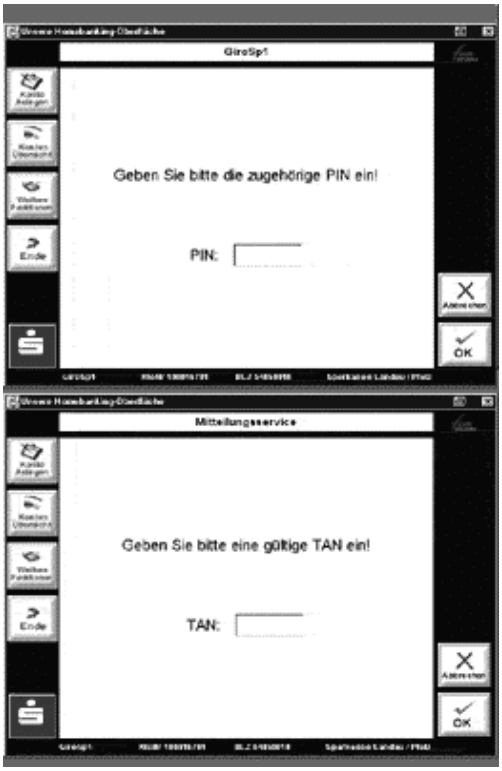
Internetbanking ist Homebanking innerhalb des digitalen Mediums Internet

Besondere Eigenschaften

Rund um die Uhr
Von zu Hause
Gewohnte Formulare

Sicherheit

Definition des Begriffes Sicherheit: Schutz der beim Zugang zum Konto und bei Vollzug der Transaktionen verwendeten Daten vor Mißbrauch



Verfahren zur Realisierung von Sicherheit

Unterscheiden von Verfahren, die Sicherheit im definierten Sinn gewährleisten:

- PIN / TAN: Verfahren, die unmittelbar an Zugang/Transaktion ansetzen
- Kryptografie: Verschlüsselung der Daten (dabei Unterscheidung von symmetrisch / asymmetrisch)

Was bedeuten die Abkürzungen PIN und TAN ?

PIN: Sicherung des Zugangs zum Konto / Abkürzung für **P**ersönliche **I**dentifikations-**N**ummer, die beim Homebanking benötigt wird, um sich als legitimer Kontoinhaber ausweisen zu können

TAN: Sicherung der Transaktion / Abkürzung für **T**rans**A**ktions**N**ummer. Diese wird beim Homebanking als Sicherheitsnachweis für eine Transaktion (z.B. Überweisung) benötigt. Nach der Transaktion wird die TAN, die vom Geldinstitut ausgegeben wird, ungültig, damit kein Mißbrauch möglich ist.

Das PIN/TAN-System wurde bei T-Online lange Zeit ohne Schadenfälle praktiziert, und beinhaltet nach heutigen Erkenntnissen kein Sicherheitsrisiko. Bedienungskomfort: aufwendig, umständlich, geringe Benutzerfreundlichkeit

Was bedeutet Kryptografie ?

Verwandeln eines Klartextes in scheinbar sinnlose Zeichenfolgen, indem beim Sender die Nachrichten mit einem Verschlüsselungs-Algorithmus chiffriert und beim Empfänger mit einem Entschlüsselungs-Algorithmus dechiffriert werden. Unterscheidung von:

- Symmetrischem Verfahren: Sender und Empfänger benutzen den gleichen Schlüssel
- Asymmetrischem Verfahren (Public-Key-Verfahren): Der Sender verwendet einen öffentlichen Schlüssel zur Chiffrierung, der Empfänger dechiffriert mit einem geheimen Schlüssel

5.3.2 Sichere Übertragung im Internet: SSL

"**(Zitat) SSL - S E C U R E S O C K E T L A Y E R** (http://www.tfh-berlin.de/~toby/vs/ssl/)

Allgemeines

TCP/IP - Neue Schichten

Sicherheit - Zertifizierung

Verschlüsselungsverfahren

symmetrischen Verfahren

asymmetrischen Verfahren

Verbindungsaufbau

zusätzliche Schicht - Public-Privat-Keys

Session key - Authentifizierung

Sicherheits-Manko

Allgemeines zu SSL

TCP/IP: Sicher und unsicher zugleich

SSL ist die Abkürzung für **S**ecure **S**ocket **L**ayer.

Mit **Layer** sind die Transportschichten angesprochen, mit denen der Datenaustausch zwischen zwei Rechner bildhaft dargestellt wird. Auf der obersten Ebene sind die Anwendungen angeordnet. Ganz unten befindet sich in dem Modell die Hardware.

Im Idealfall lassen sich sieben Schichten definieren, denen sich wiederum im Idealfall jeweils ein Protokoll oder Programm zuordnen läßt. Alle Schichten tragen dazu bei, den Datenfluß zwischen den beiden Rechnern sicherzustellen.

Im wirklichen Leben paßt das Modell nicht immer so ideal. Das Übertragungsprotokoll TCP/IP deckt mit seinen zwei Komponenten (TCP und IP) mindestens vier Schichten ab. Das Protokoll ist eine Art Esperanto in der Rechnerwelt. Mit Ausnahme der Zuse-Rechner und des ZX81 unterstützen wohl alle Rechner und Betriebssysteme TCP/IP. Es ist einfach zu implementieren, robust und sicher -- betriebssicher.

Als TCP/IP vor fast 30 Jahren erfunden wurde, stand vor allem die Absicht im Vordergrund, eine ausfallsichere und stabile Verbindung mit hoher Betriebssicherheit zu schaffen. Die Sicherheit und Authenzität der übermittelten Daten spielte eine untergeordnete Rolle.

Neue Schichten

Mit TCP/IP war der Wunsch nach sicheren Verbindungen im Sinne von Datensicherheit nicht zu verwirklichen. Ohne TCP/IP gibt es kein Internet.

Die Firma Netscape löste das Problem auf folgende elegante Weise: Die Entwickler erweiterten TCP/IP um zwei weitere Schichten.

SSL Record Protokoll
SSL Handshake Protocol

Das erklärt auch die Bezeichnung "Layer"; sie liegen funktional zwischen dem Aufgabenbereich von TCP/IP und den Anwendungen. Diese beiden Schichten liegen bildlich betrachtet unmittelbar aufeinander und werden darum von einigen Autoren auch als eine einzige Schicht angesprochen. Obgleich sich in diesen beiden Schichten während einer sicheren Verbindung allerlei Software-Know-How austobt, ist sie für die angrenzenden Schichten transparent: Weder die Anwendung (der Browser), noch die unter der dem SLL-Protokoll liegende Transportschicht bemerken das Wirken des SLL-Protokoll. Im **Klartext**: SSL erfordert weder massive Änderungen vorhandener Anwendungen noch neue Transportprotokolle.

Während einer sicheren Verbindung kommunizieren die beteiligten Rechner ausschließlich über den Mechanismus, der von SSL bereit gestellt wird. Steht die sichere Verbindung nicht zur Verfügung, schaltet sich das SSL-Protokoll gleichsam aus.

Sicherheit durch SSL

Das SSL-Protokoll schafft unter drei Gesichtspunkten sichere Verbindungen:

1. Die Verbindung ist im besten Sinne privat, weil ihr Inhalt nur verschlüsselt über das Netz geht.
2. Die Identität des Servers steht fest.
3. Wirkungungsvolle Algorithmen prüfen, ob die Daten vollständig und unverändert ihren jeweiligen Empfänger errreichen.

Das SSL-Protokoll wird dadurch initiiert, dass dem bekannten http ein s angehängt wird: http**s**://www.ssl.de.

Das ist für den **Browser** der Anlaß, vom angesprochenen Server ein **Zertifikat** und seinen **öffentlichen Schlüssel** abzufordern. Dieser Schlüssel wird zusammen mit einer Prüfsumme und einer ID an den Browser zurückgemeldet. Diese Informationen werden von einigen wenigen Zertifizierungsfirmen errechnet. Die bekannteste ist VeriSign; Dieser Zertifizierungspro-

zeß ist gleichermaßen zeitaufwendig wie Kostenintensiv und speziell für Anwender, die nicht in den USA wohnen, mit einigen Problemen behaftet.

Der **Browser** prüft anhand der übermittelten Daten, **ob er wirklich** mit dem Server verbunden ist, der in der URL angegeben ist. Ist das der Fall, gibt der Browser dem Anwender eine entsprechende Information: Beim Internet Explorer schließt sich das Bügelschloß, der Navigator/Communicator signalisiert eine sichere Seite durch den intakten Schlüssel.

In der folgenden Phase **verständigen** sich die **beiden** Rechner auf einen **symetrischen Schlüssel** (Session Key). Da diese Absprache in asymetrischer Verschlüsselung vollzogen wird, ist die Sicherheit gegeben. Der Browser schickt dem Server vor dem Beginn des eigentlichen Datenaustausches einige **Testnachrichten**, die der Server nur beantworten kann, wenn es **wirklich** der Server ist, der er zu sein vorgibt.

Zertifizierung

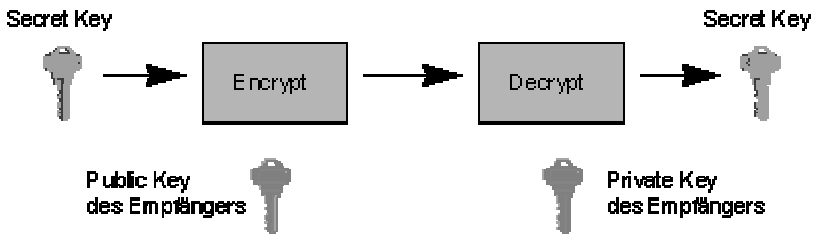
Im Zentrum des SSL-Protokoll steht das digitale Schüsselpaar aus öffentlichem und privaten Schlüssel des Servers sowie die ID der Zertifizierungsstelle. Jeder virtueller Websserver benötigt ein eigenes Schlüsselpaar, weil bei der ID unter anderem der Domain-Namen einfließt.

Verschlüsselungsverfahren

Symmetrische Verfahren

Bei der Secret Key Encryption verwenden beide Kommunikationspartner bei der Verschlüsselung einen **gemeinsamen** "geheimen" Schlüssel verwenden. **Ist** dieser Schlüssel einem dritten **bekannt**, **kann** auch dieser die ausgetauschten Nachrichten entziffern. Aus diesem Grunde werden Secret Key Encryption Verfahren auch als **symmetrische** Verschlüsselungsalgorithmen bezeichnet. Das bekannteste Secret Key Encryption Verfahren ist der DES-Algorithmus.

Secret Key (symmetrische) Verschüsselungsverfahren sind im Vergleich zu asymmetrischen Verfahren wesentlich kompakter und effizienter. Aus diesem Grunde erfolgt die Verschlüsselung der Nachrichten i. d. R. **mittels symmetrischer Algorithmen**, **deren Keys** (Session Keys) *unter Anwendung von Public Key (asymmetrischen) Verfahren* in der gleichen Nachricht oder in separaten Dialogen **ausgetauscht werden** .



Aufgrund von Lizenzrechten und US-Gesetzesregelungen werden international meistens nur symmetrische Verschlüsselungsverfahren mit einer Schlüssellänge von 40 oder 56 bit eingesetzt, obwohl hierdurch keine ausreichende Sicherheit mehr gewährleistet werden kann. Eine Schlüssellänge von 128 bit gilt bei symmetrischen Verfahren allgemein als ausreichend sicher.

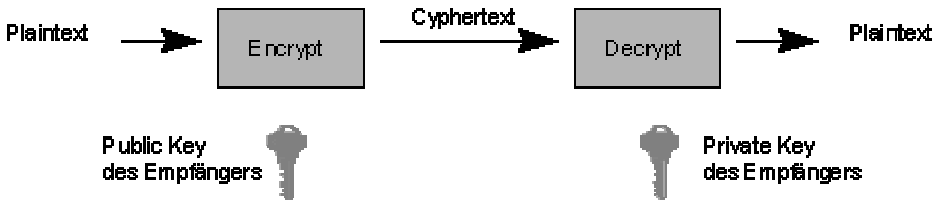
Asymmetrische Verfahren

Public Key Kryptographie darf als die Basis aller Sicherheitsmaßnahmen im Electronic Commerce angesehen werden.
Public Key Verschlüsselungsverfahren sind **asymmetrische** Verfahren und operieren mit **2 Schlüsseln** - einem **Private** Key und einem **Public** Key -, die **zusammen** generiert werden. Der Private Key ist **geheimzuhalten** und sollte **nur** seinem Besitzer zugänglich sein, während der **Public** Key allgemein verteilt werden kann und z. B. in der Zeitung veröffentlich werden könnte ("Öffentliche Bekanntmachung: Sollten **Sie** "Mersch Online" eine Nachricht **zukommen lassen** wollen, **verschlüsseln Sie** sie bitte mit dem (Public-)Key '0AW4.....XD3'").

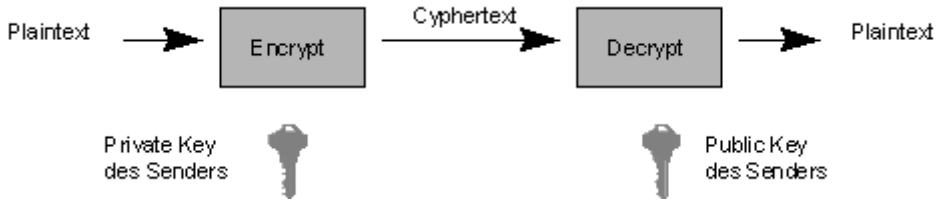
Die **Grundannahme** der Public Key Kryptographie - und damit des gesicherten Electronic Commerce - **ist**, daß der **Private Key** nur mit unverhältnismäßig **hohem** Aufwand **aus** dem **Public Key** erzeugt werden kann. Heutige Schätzungen gehen meist - in Abhängigkeit der Key-Länge - von einem Aufwand von mehreren Millionen Jahren Rechenzeit aus.

Der bekannteste Public Key Verschlüsselungsalgorithmus ist **RSA** (von Rivest, Shamir und Adleman). Für diesen gilt:

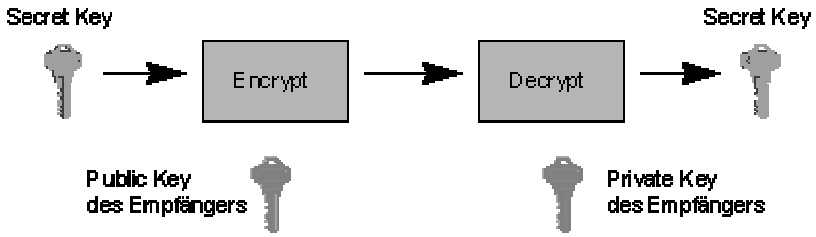
- **Mit** dem **Public Key ver**schlüsselte Nachrichten können mit dem zugehörigen **Private Key ent**schlüsselt werden. (Mit dem public key von Mister X kann ich (und jederman) eine Nachricht schreiben, die NUR Mister X lesen kann. ["Nachricht nur für..." ist gesichert])



- Mit dem **Private Key ver**schlüsselte Nachrichten können mit dem zugehörigen **Public Key en**tschlüsselt werden. (Mit dem public key von Mister X kann ich Nachrichten lesen, die NUR VON Mr. X stammen können ["Nachricht nur von..." ist gesichert])



Asymmetrische Verschüsselungsverfahren sind im Vergleich zu symmetrischen Verfahren langsam und rechenintensiv. Aus diesem Grunde erfolgt die Verschlüsselung der Nachrichten i. d. R. mittels symmetrischer Algorithmen, deren Keys (Session Keys) unter Anwendung von Public Key Verfahren in der gleichen Nachricht oder in separaten Dialogen ausgetauscht werden:



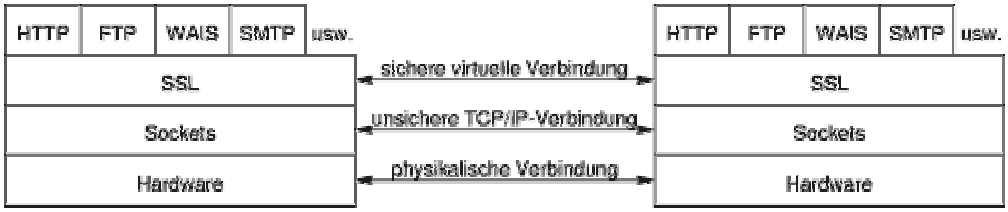
Das Anwendungsspektrum asymmetrischer Verschlüsselungsverfahren geht weit über das reine Verschlüsseln von Nachrichten hinaus und ist wahrscheinlich noch bei weitem nicht ausgeschöpft.

Public-Key-Verschlüsselungsverfahren gelten bei Schlüssellängen von 1024 bit oder idealerweise 2048 bit als ausreichend sicher.

Verbindungsaufbau

S E C U R E S O C K E T L A Y E R

SSL legt, wie der Name andeutet, eine **zusätzliche** Schicht **zwischen** die zuverlässige Transport-Ebene TCP/IP und die Anwendungsebene (HTTP, Telnet, FTP,...). Von "oben" gesehen ist sie transparent, d.h. die Anwendungsprogramme können ohne große Modifikation auf eine sichere Übertragung zugreifen. Für die Transportschicht erscheint SSL hingegen als An-



wendungsebene:

Der Verbindungsaufbau läuft in vier Schritten ab:

1. In der sogenannten Hello-Phase baut der Client eine Verbindung zum Server auf und teilt ihm mit, welche Kryptographie-Algorithmen er unterstützt.
2. Der Server wählt daraus ein **Public-Key-**, ein **Privat-Key-** und ein **Hash-Verfahren** aus und teilt sie dem Client mit. Gleichzeitig sendet der Server ein **Zertifikat**, das unter anderem den **öffentlichen Schlüssel** des Servers enthält. (Mit Hilfe des Zertifikats kann der Client überprüfen, ob die Antwort tatsächlich vom gewünschten Server stammt.)
3. Der Client generiert einen **Sitzungsschlüssel** (Session key) für einen Datenaustausch per Private-Key-Verfahren. Aus Geschwindigkeitsgründen werden standardmäßig symmetrische Verfahren verwendet (hier: RC4). Der dazu notwendige Schlüsselaustausch wird durch Verschlüsselung mit den in den Zertifikaten enthaltenen öffentlichen Schlüsseln geschützt. Diesen chiffrierten Schlüssel schickt der Client an den Server.
4. In der abschließenden **Authentifizierung**s-Phase authentifiziert der Client den Server, indem er ihm eine Reihe von mit dem Sitzungsschlüssel chiffrierten zufälligen **Testnachrichten** schickt, die der Server nur dann korrekt dechiffrieren und bestätigen kann, wenn es sich um den "echten" Server handelt.

   In einem optionalen Schritt kann der Server auf vergleichbare Weise den Client authentifizieren. Die Client-Authentifikation funktioniert nur dann, wenn der Client über ein offiziell registriertes Zertifikat verfügt.

Damit ist der **initiale Verbindungsaufbau abgeschlossen**. Anschließend können die eigentlichen Daten geschützt übertragen werden.

Die Verschlüsselung im Einzelnen

Die zu übertragenden Daten werden in **kleine Blöcke** geteilt, die auch noch komprimiert werden können, was die Schnelligkeit und auch die kryptographische Sicherheit weiter erhöht. Die **Blocknummer wird hinzugefügt** und mittels Hash-Funktion eine **Prüfsumme** angehängt.Abschließend wird mit dem **symmetrischen Verfahren**, üblicherweise dem schnellen Stromchiffrierer RC4, verschlüsselt.

Sollten beim Empfang Ungereimtheiten auftreten (falsche Prüfsummen), wird dies auf eine versuchte Manipulation zurückgeführt, da dem Übertragungsprotokoll TCP/IP vertraut wird. Daraufhin wird eine verschlüsselte Fehlernachricht versandt und die Verbindung abgebrochen.

Sicherheits-Manko: US-Export-Restriktionen

Netscape hat SSL in den Navigator eingebaut und vertreibt mit dem Netscape Secure Server das entsprechende Gegenstück. "**Secure**" ist die Übertragung allerdings nur mit der in den USA vertriebenen Variante der Software. Die restriktive US-Exportpolitik verhindert eine gute Verschlüsselung außerhalb der USA, da Netscape, um eine Exportlizenz zu erhalten, den **Sitzungsschlüssel nicht in voller Länge chiffriert** übertragen darf. Lediglich eine Chiffrierung von mageren 40 Bit des Schlüssels ist erlaubt.

Dies macht Angriffe auf die Sitzungsschlüssel möglich:
In mehreren Fällen wurde bereits über ein Cluster vernetzter Workstations, die den gesamten (Rest-)Schlüsselraum per "brute force" absuchten, das Ergebnis nach ein bis zwei Wochen gefunden! Eine zweite Herausforderung knackten die "Cyperpunks" innerhalb von knapp zweiunddreißig Stunden mit einem "Key cracking ring". Dieses Verfahren beruht ebenfalls auf brute force, verteilt die Aufgabe aber auf beliebig viele Maschinen im Internet, die dazu lediglich ihre freie CPU-Zeit zur Verfügung stellen müssen. (Zitat Ende)"

5.3.3 eCash: Auszüge aus einem Vortrag zum Thema eCash

Aus einem Vortrag zum Theme Verschlüsselung und eCash (Quelle: http://www.remote.org/frederik/projects/cash/):

5.3.3.1 Einleitung

In diesem Beitrag geht es um das Konzept einer digitalen "Signatur", also dem Äquivalent zu einer Unterschrift auf einem Auftrag. Wie im heutigen Bankgewerbe die "physische" Unterschrift spielen Signaturen in den meisten eCash-Systemen eine wichtige Rolle. (...) Gegen Ende des Vortrags werden wir aus den vorgestellten Bausteinen einige einfache eCash- Verfahren konstruieren und untersuchen, inwiefern diese bereits den diversen Anforderungen an digitales Geld genügt.

5.3.3.2 Signaturen

Eine Signatur dient vor allem dazu, zweifelsfrei zu beweisen, daß eine bestimmte Person ein Dokument unterzeichnet bzw. ausgefertigt hat.

Anforderungen an Signaturen
Von einer Unterschrift oder Signatur erwartet man eine Reihe von speziellen Eigenschaften:

- Die Signatur soll authentisch sein:
  Sie ist ein Zeichen dafür, daß der Unterschreibende das Dokument persönlich und absichtlich unterschrieben hat.
- Die Signatur soll nicht fälschbar sein.
- Die Signatur soll nicht wiederbenutzbar sein:
  Sie ist Teil des Unterschriebenen; man kann sie nicht auf ein anderes, nie unterschriebenes Dokument übertragen.
- Das Unterschriebene ist nicht veränderbar:
  Nach erfolgter Unterschrift kann keine Änderung am Text mehr erfolgen.
- Die Signatur kann nicht abgestritten werden:
  Niemand kann nachher behaupten, der Unterschriftsapparat sei ihm abhanden gekommen.

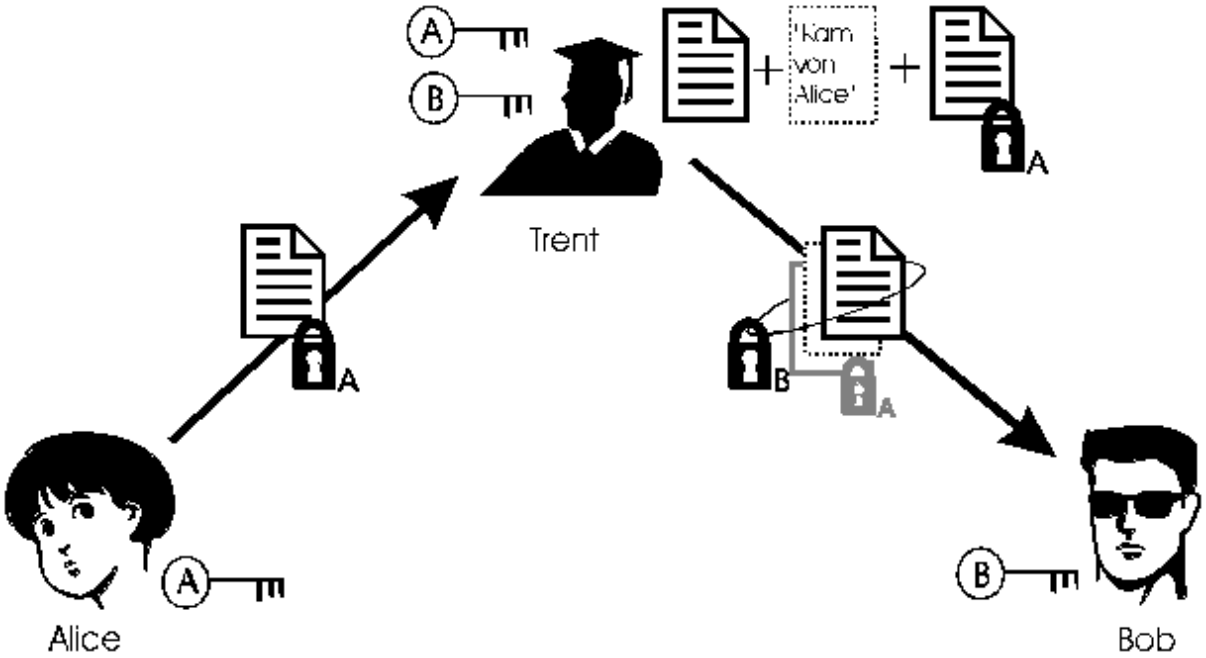
Es ist nicht schwer zu erkennen, daß die meisten dieser Eigenschaften von den heute verbreiteten "physischen" Signaturen nicht voll erfüllt werden; so ist es zum Beispiel relativ leicht, eine Unterschrift auszuschneiden und unter ein anderes Dokument zu plazieren, das Unterschriebene im Nachhinein zu verändern oder auch den Finanzbehörden glaubhaft zu machen, man habe nicht gewußt, was mit der eigenen Unterschriftsmaschine alles unterzeichnet wurde.

Wir werden zu prüfen haben, inwiefern die digitalen Signaturen in diesen Punkten an die Sicherheit der heute verbreiteten Unterschrift heranreichen oder diese sogar übertreffen.

Signatur mit symmetrischen Kryptoverfahren und einem vertrauenswürdigen Dritten
Die einfachste denkbare Signatur basiert auf symmetrischen Kryptoverfahren und einem "vertrauenswürdigen Dritten", der in der englischsprachigen Literatur meist "Trent" genannt wird (für "Trusted Arbitrator").

Trent ist im Besitz aller geheimen Schlüssel. Möchte Alice nun Bob glaubhaft versichern, daß ein bestimmtes Dokument von

ihr ist, verschlüsselt sie es und sendet es an Trent. Dieser entschlüsselt es mit Alices Schlüssel und weiß daraufhin, daß es tatsächlich von Alice gekommen sein muß (sonst wäre die Entschlüsselung fehlgeschlagen). Er zertifiziert diesen Tatbestand in einer separaten Nachricht ("Das anliegende Dokument habe ich von Alice erhalten"), verschlüsselt beides mit Bobs Schlüssel und sendet es an Bob.
Bob wiederum kann sicher sein, daß die Nachricht von Trent kam, denn nur Trent und Bob selbst kennen den Schlüssel. Da Bob Trent vertraut, nimmt er aufgrund von Trents angehängter Nachricht nun an, daß das erhaltene Dokument ursprünglich von Alice kam.



Dieses Verfahren erinnert an zuweilen übliche notarielle Unterschriftsbeglaubigungen, bei denen der Notar als "vertrauenswürdiger Dritter" bestätigt, daß die Unterschrift unter einem Dokument tatsächlich von einer bestimmten Person, die sich ihm ausgewiesen hat, ist.

Die *Authentizität* und *Nichtfälschbarkeit* sind hier trivialerweise erfüllt, da jeweils nur die Beteiligten und der vertrauenswürdige Trent den untereinander benutzten Schlüssel kennen; nur Alice kann also das Urpsrungsdokument verschlüsselt haben, nur Trennt kann die Nachricht an Bob abgesandt haben, und Bob glaubt Trent dessen Zertifikat "dies erhielt ich von Alice".

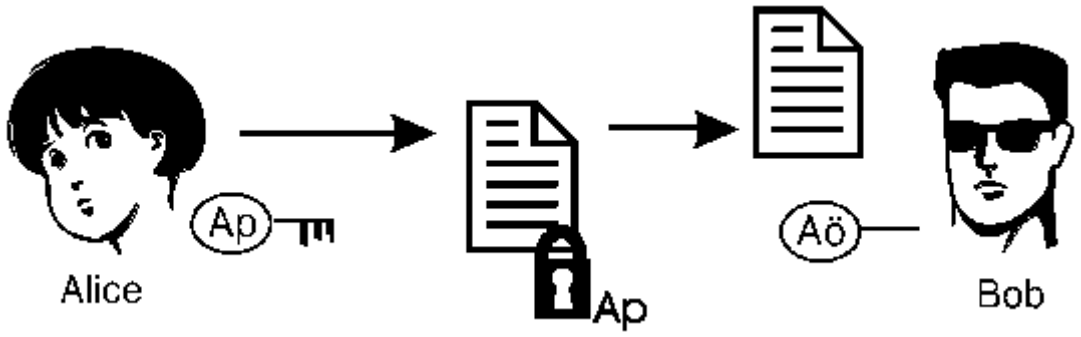
Für die anderen drei Kriterien ist es von Bedeutung, daß Bob zusätzlich von Trent das mit Alices Schlüssel verschlüsselte Originaldokument erhält. Mit diesem kann er zwar nichts anfangen, aber es gewährleistet die *Nichtabstreitbarkeit:* Behauptet Alice später, das Dokument nie abgesandt zu haben, so müssen sie oder Trent in einer Gerichtsverhandlung das bei Bob gelagerte, verschlüsselte Dokument entschlüsseln, und es ergibt sich, daß es tatsächlich mit dem Schlüssel A verschlüsselt war, also von Alice kam. Die *Nichwiederbenutzbarkeit* der Unterschrift bzw. *Unveränderbarkeit* des Dokuments sind ebenfalls dadurch gewährleistet: Wenn Bob eine Änderung am Dokument vornimmt und nun behauptet, das geänderte Dokument von Alice über Trent erhalten zu haben, wird Alice Einspruch einlegen. Bob muß nun in der Lage sein, das verschlüsselte Dokument vorzuweisen, und nach der Entschlüsselung mit dem Schlüssel A zeigt sich, daß das Ergebnis nicht identisch ist mit dem, was Bob erhalten zu haben vorgab.

Die Nichtabstreitbarkeit ist natürlich nur in Grenzen gewährleistet. Ebenso, wie es möglich ist, eine physische Unterschrift dadurch abzustreiten, daß man behauptet, der eigene Unterschriftsapparat oder -Stempel sei mißbraucht worden, kann man auch "versehentlich" seinen geheimen Schlüssel veröffentlichen oder verlieren, und schon kann jedes signierte Dokument theoretisch von jedermann kommen. Es gibt jedoch erweiterte Protokolle, die nicht diesem Manipulationsrisiko ausgesetzt sind.

Signatur mit Public-Key-Verfahren

Bisher wurde im Rahmen dieses Seminars nur auf den Einsatz der Public-Key-Kryptographie zur Verschlüsselung von Nachrichten an einen bestimmten Empfänger eingegangen: Möchte Alice Bob ein Dokument senden, das sonst niemand lesen kann, so verschlüsselt sie es mit Bobs öffentlichem Schlüssel; nur der Inhaber von Bobs privatem Schlüssel - also Bob - kann die Nachricht lesen. Über den *Absender* ist damit jedoch nichts gesagt; die Nachricht kann von jedem kommen, der Bobs öffentlichen Schlüssel kennt.

Public-Key-Kryptographie ist jedoch auch zum Signieren von Dokumenten geeignet. Hierbei verschlüsselt Alice eine Nachricht mit ihrem privaten Schlüssel. Jeder, der Alices öffentlichen Schlüssel kennt, kann diese Nachricht lesen und weiß im selben Augenblick, daß sie von Alice kommen muß, da niemand sonst Nachrichten erzeugen kann, die nach der Entschlüsselung mit Alices öffentlichem Schlüssel Sinn ergäben.



Bei diesem Verfahren sind *Authentizität* und *Nichtfälschbarkeit* ebenfalls trivialerweise erfüllt, da nur Alice selbst ihren geheimen Schlüssel kennt und jede Nachricht, die sich mit ihrem öffentlichen Schlüssel entschlüsseln läßt, daher von ihr kommen muß. Auch die *Unveränderbarkeit* ist gewährleistet, denn wenn Bob die erhaltene Nachricht verändert, paßt Alices öffentlicher Schlüssel nicht mehr, und jeder kann das feststellen.

Für die *Nichtwiederverwendbarkeit* der Unterschrift unter anderen Dokumenten gilt dasselbe; es ist für Bob jedoch möglich, einfach zu behaupten, er habe dasselbe Dokument (beispielsweise eine Bestellung) zehnmal (statt nur einmal) erhalten. Um dem vorzubeugen, könnte Alice eine Datums- und Zeitangabe oder eine laufende Nummer in alle von ihr versandten Dokumente einbauen.
Für die *Nichtabstreitbarkeit* gilt, was auch schon im vorigen Abschnitt gesagt wurde; Alice kann nicht abstreiten, daß die Mitteilung von ihr kam, es sei denn, sie behauptet, ihr Schlüssel sei ihr abhanden gekommen.

5.3.3.3. Electronic Cash

Aus den in diesem Vortrag vorgestellten Konzepten einer "Signatur" lässt sich bereits funktionierende eCash-Systeme entwikkeln. Zuvor seien jedoch die wünschenswerten Eigenschaften elektronischen Geldes zusammengefaßt:

- Unabhängigkeit:
  Das Geld darf nicht an einen physischen Ort gebunden sein und muß immateriell - z.B. im Internet - übertragbar sein.
- Sicherheit:
  Das Geld darf nicht fälsch- bzw. kopierbar sein.
- Schutz der Privatsphäre:
  Wie beim Bargeld soll niemand feststellen können, wer welche Geldeinheit wann wo ausgegeben hat.
- Offline-Fähigkeit:
  Wird das Geld ausgegeben, ist in diesem Augenblick keine Verbindung zu einem Zentralrechner (z.B. der Bank) notwendig.
- Übertragbarkeit:
  Das Geld soll frei auch zwischen Personen übertragbar sein, d.h. der Weg "Bank-Käufer- Verkäufer-Bank" darf nicht vorgeschrieben sein.

- Teilbarkeit:
  Das Geld soll beliebig in kleinere Einheiten aufgeteilt werden können.

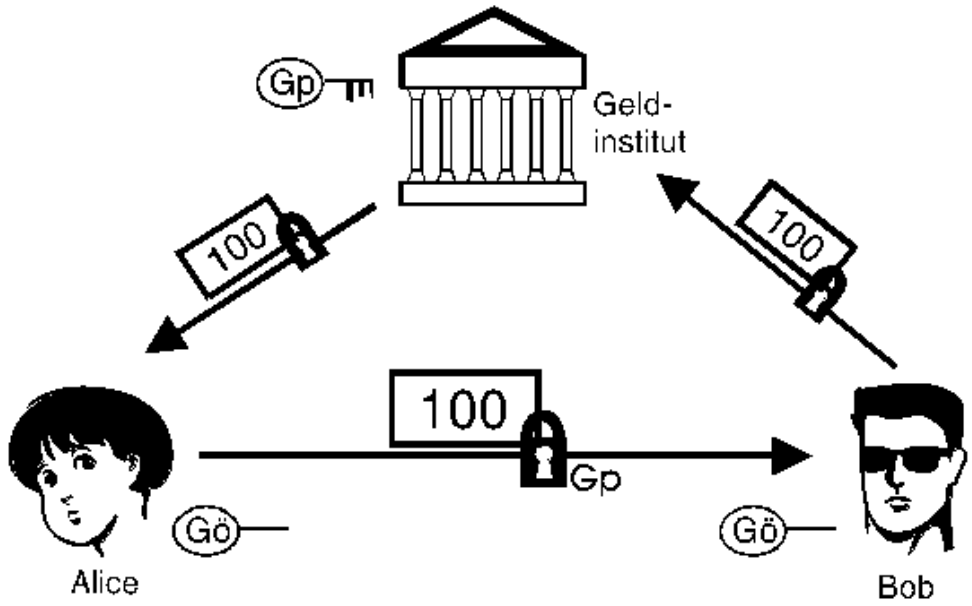
Dies sind *wünschenswerte* Eigenschaften. In diesem Vortrag werden wir kein eCash-Verfahren vorstellen können, das allen diesen Forderungen genügt.

Das einfachste digitale Geld

Zum Einstieg in das Thema stellen wir zunächst ein ganz einfaches Verfahren für digitales Geld vor. Wir verwenden dabei die Begriffe "Zettel" und "aufschreiben", weil das Beispiel so anschaulicher wird; tatsächlich "digital" wird das Geld natürlich nur, wenn man eine elektronische Form der Nachrichtenspeicherung und -Übermittlung benutzt. Alle Protokolle funktionieren selbstverständlich auch papierlos.

Alice fordert von der Bank einen Geldschein an.

- Die Bank schreibt auf einen Zettel "Dies sind DM 100,-" und signiert den Zettel, indem sie ihn (oder eine Hashfunktion davon) mit ihrem privaten Schlüssel verschlüsselt. Gleichzeitig bucht sie DM 100,- von Alices Konto ab.
- Alice besitzt jetzt einen "Geldschein" und trägt ihn zu Bob in den Laden (sie kauft Band 1 von D.E. Knuths "The Art of Computer Programming" im Sonderangebot).
- Bob prüft den "Schein", indem er ihn mit dem öffentlichen Schlüssel der Bank entschlüsselt. Es klappt, also weiß Bob, daß der Schein tatsächlich von der Bank verschlüsselt bzw. signiert wurde und daher "echt" ist.
- Bob reicht den Zettel bei der Bank ein; diese erstattet ihm die DM 100,- auf sein Konto.



Bei diesem simplen Verfahren tritt zunächst das Problem auf, daß Alice und Bob beliebig viele Kopien des Scheins anfertigen und ausgeben können. Die Bank muß also eine eindeutige "Seriennummer" einführen, die sie auf alle Scheine druckt.

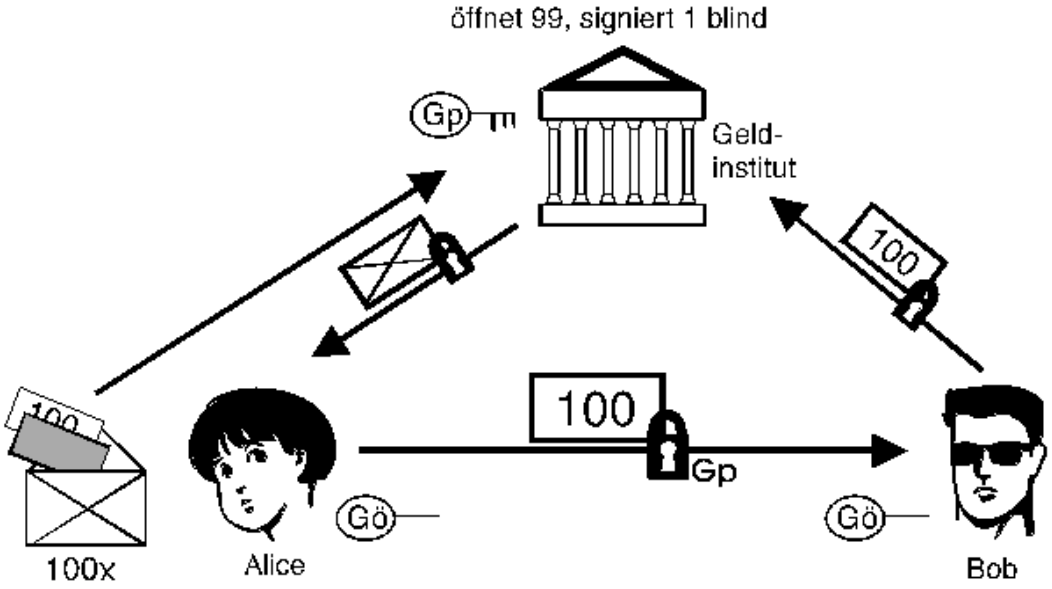
Dadurch entstehen jedoch zwei neue Probleme:

- Die Bank kann, wenn Bob den Geldschein einreicht, feststellen, daß er von Alice kam. Ist Alice Ordensschwester und Bob Inhaber eines zwielichtigen Video-Shops, sammelt sich bei der Bank schnell brisante Information an. Diese Information wird zwar heute bei bargeldlosem Zahlungsverkehr auch gespeichert, ist jedoch gesellschaftlich problematisch und sollte, wenn sie nicht zur technischen Abwicklung nötig ist, gar nicht erst erzeugt werden.
- Das Geld ist nicht "Offline-fähig", denn Bob weiß nicht, ob Alice denselben Schein evtl. schon woanders ausgegeben hat und die Bank seine Einlösung daher platzen läßt. Bob muß sofort bei der Einlösung des Scheins bei der Bank rückfragen, ob diese Seriennummer tatsächlich noch nicht eingelöst wurde.

Digitales Geld mit "Blinding Factor"

Der "Blinding Factor", den wir nun einführen wollen, ist eine erstaunliche Idee, die aber bei genauerem Hinsehen durchaus gut funktioniert. Wieder ziehen wir für unser Beispiel (genauer gesagt, ein Beispiel von David Chaum, dem Erfinder des "Blinding") Umschläge und Zettel heran.

- Alice schreibt auf 100 Zettel: "Dies sind DM 100,- ", und versieht jeden mit einer Seriennummer, die so lang, ist, daß die Wahrscheinlichkeit, daß jemand anders dieselbe benutzt, sehr gering ist.
- Sie verpackt alle 100 Zettel in Umschläge und legt jeweils noch ein Kohlepapier ein.
- Alices Bank öffnet 99 von den 100 Umschlägen und vergewissert sich, daß Alice nicht gelogen hat. War Alice in 99 Fällen ehrlich, nimmt die Bank an, daß auch im 100. Umschlag das Richtige steht, unterschreibt blind (=> Bank kennt nicht die Seriennummer des Geldscheins!) den 100. Umschlag und bucht DM 100,- von Alices Konto ab.
- Alice kann den Geldschein wie vorher ausgeben.
- Die Bank löst später den Schein ein, ohne zu wissen, daß er von Alice kommt. (D.h. Bank erkennt zwar die eigene Signatur, sieht aber die (von Alice erstellte) Seriennummer zum ersten Mal!)Wenn der Schein mit der gleichen Seriennummer bereits eingelöst wurde, weist die Bank ihn zurück.

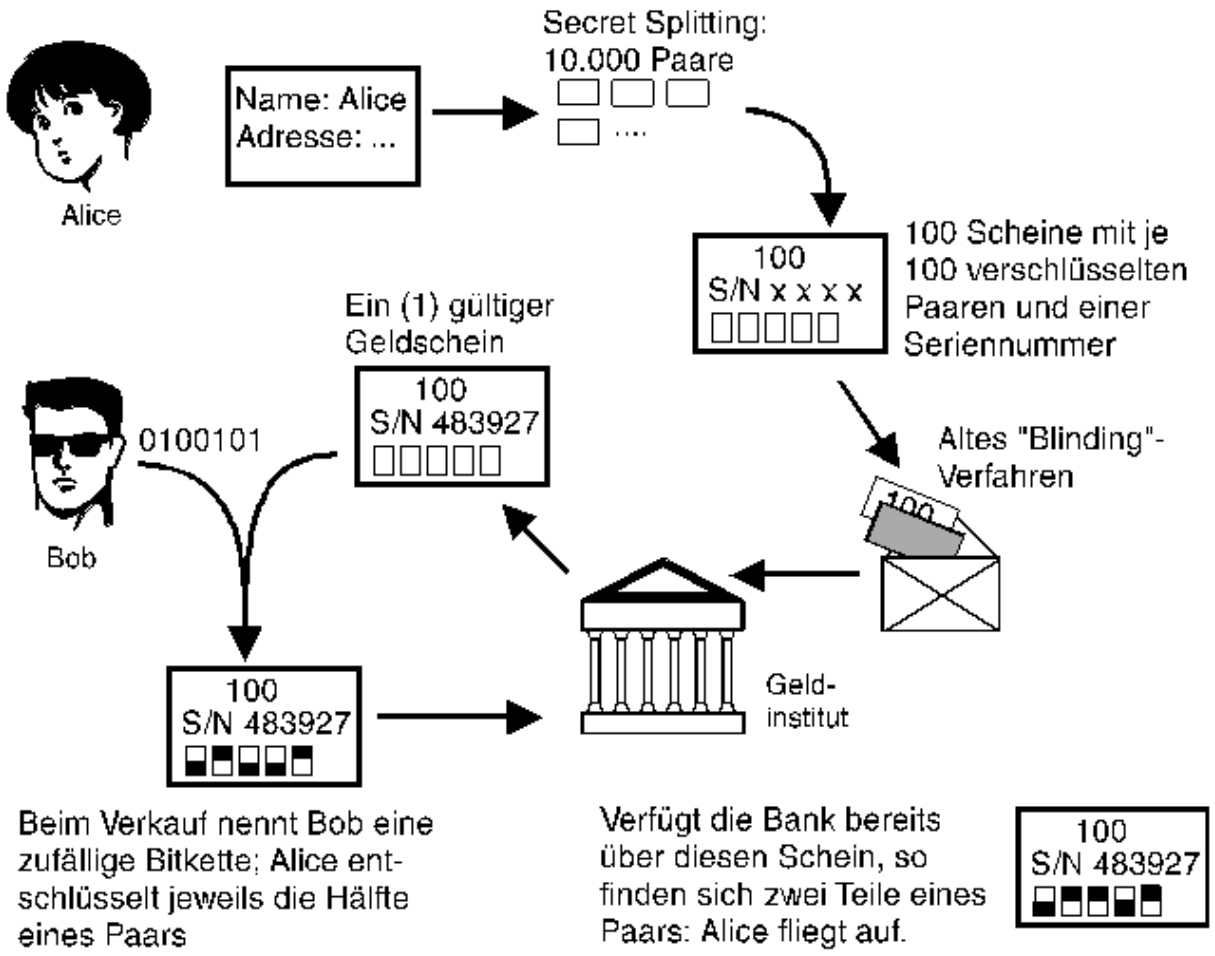


Diese Protokoll löst das Problem der Verfolgbarkeit; Alice kann nun ihr Geld ausgeben, ohne daß jemand später weiß, wo das geschah. "Offline-fähig" ist das neue Geld aber immer noch nicht, denn es ist nicht sichergestellt, daß Alice den gleichen Geldschein nicht mehrmals ausgibt. Auch Bob könnte das tun, und dann wäre nicht einmal klar, ob Alice oder Bob nun falsch spielen. Daher muß wie zuvor beim Bezahlen bereits die Bank gefragt werden, ob dieser Schein noch gültig ist.

Digitales Geld mit Schutz vor Mehrfach-Ausgabe

Zur Absicherung gegen das mehrfache Ausgeben desselben Geldscheins müssen wir zunächst ein neues Konzept einführen: Das sogenannte "Secret Splitting". Beim "Secret Splitting" wird eine Nachricht in beliebig viele einzelne Teile zerlegt und ist nur dann wieder lesbar, wenn man alle Teile besitzt. Dabei ist durch Kryptographie sichergestellt, daß man nicht, wie etwa bei einem zerissenen Blatt Papier, aus Teilen der Nachricht auf das Ganze schließen kann.

Wir sind nun an einem Punkt, an dem die "Papier-Analogie" nicht mehr hundertprozentig greift, weil inzwischen solche Datenmengen erzeugt werden müssen, daß niemand sie mehr auf einen Zettel schreiben kann; dennoch halten wir noch einmal daran fest. Alice erzeugt für dieses Protokoll zunächst eine Information I, die ihre Identität verrät, z.B. "Ich bin Alice Ryder und wohne in der Bahnstraße 28 in 12345 Berlin". Mit einem Secret-Splitting-Protokoll erzeugt sie hieraus 10.000 mal ein Tupel (I1, I2)x. Kennt man zwei zusammengehörige I, kann man die Original-Information lesen; sonst nicht. (Also immer a1 & a2 (oder b1 & b2 oder c1 & c2 usw.) **zusammen** ergeben die Informarion, aber z.B. a1 & c2 ergibt garnichts, d.h. es müssen immer die **beiden** Hälften **eines** Paares sein)



- Alice erzeugt wie gehabt 100 Zettel mit 100 Seriennummern. Zusätzlich schreibt sie auf jeden Zettel die beiden Hälften von 100 I-Paaren in verschlüsselter Form.
- Sie verpackt, ebenfalls wie vorher, alle 100 Zettel in Umschläge und legt jeweils noch ein Kohlepapier ein.
- Alices Bank öffnet 99 von den 100 Umschlägen und vergewissert sich, daß Alice nicht gelogen hat; dazu muß Alice die I-Paare auf allen 99 Zetteln entschlüsseln, damit die Bank sieht, daß (bei allen 9900 Paaren!) tatsächlich die richtige Identität herauskommt. Ist das der Fall, unterschreibt sie blind den 100. Umschlag und bucht DM 100,- von Alices Konto ab.
- Alice kann den Geldschein, der nun 100 verschlüsselte I-Paare enthält, wie vorher ausgeben. Der Händler Bob bittet sie dabei, aus **jedem** der 100 I-Paare je **eine** Hälfte (pro Paar immer nur eine der beiden) zu entschlüsseln (welche Hälfte, legt der Händler anhand eines Zufallsgenerators fest). Bob **kann** zwar nachvollziehen, ob die Entschlüsselung **richtig** vorgenommen wird (ob Alices Schlüssel "paßt", weil sonst "Error"-Meldung), kann mit den dadurch entstehenden unverschlüsselten Hälften jedoch **nichts** anfangen, da er wegen des "Secret Splitting" **auch** die **zweite** Hälfte, die ja noch verschlüsselt ist, benötigt.
- Die Bank löst später den Schein ein, ohne zu wissen, daß er von Alice kommt.
- Wenn Alice versucht, den Schein mehrfach auszugeben, fällt dies in dem Moment auf, in dem Bob den Schein einlöst. Die Bank merkt das an der gleichen Seriennummer und holt den bereits eingelösten Schein aus der Datenbank. Dann vergleicht sie die I-Paare beider Scheine. Die Wahrscheinlichkeit, daß jew. pro Paar **genau** die **gleichen** Hälften auf beiden Scheinen "geöffnet" (entschlüsselt) sind, ist **sehr gering**. Viel wahrscheinlicher ist, daß der Händler, bei dem Alice den Schein **vorher** bereits ausgegeben hat, sie bei **mindestens einem** I-Paar eine **andere** Hälfte öffnen ließ. Dadurch hat die Bank nun aber von **diesem** I-Paar **beide** Hälften, kann sie **zusammensetzen** und erhält **Alices Identität** - eine halbe Stunde später steht bereits die Polizei vor ihrer Tür. Wie man sieht, *verhindert* dieses Verfahren nicht, daß ein Geldschein mehrfach ausgegeben wird - aber es stellt sicher, daß die Übeltäterin zur Verantwortung gezogen werden kann, wenn sie es probiert.