Electronic Commerce

(Facharbeit im Fach politische Bildung)

Schule:

Schuljahr:

Kurs:

Fach:

Name:

Thema: *Electronic Commerce*

Name (Fachlehrerin):

Ausgabetermin des Themas:

Abgabetermin der Arbeit:

---------- ----------
(Unterschrift Schüler) **(Unterschrift Fachlehrerin)**

Die vorliegende Arbeit wurde am :_____ eingereicht.

Note: _____ / _____ Punkte

_____
(Unterschrift Fachlehrerin)

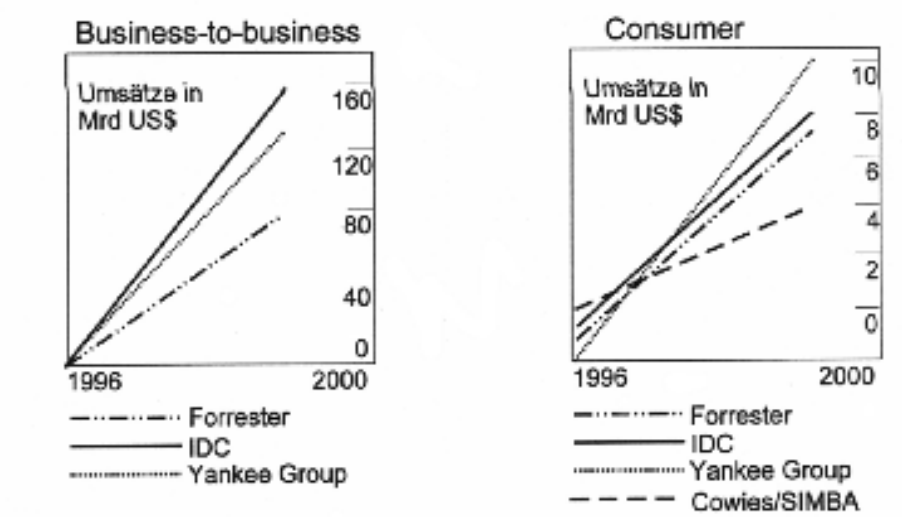
Inhaltsverzeichnis

1 Einführung

Der elektronische Markt und der Handel über das Internet ist momentan in der Presse und in vielen anderen Medien das Thema Nummer 1. Auch auf der CEBIT im März 2000 war Electronic Commerce unter vielen anderen Neuerungen das am stärksten vertretene Thema. Dennoch verhält sich der Handel, aber auch die Konsumenten diesem Thema gegenüber eher zurückhalten. Ein Grund hierfür mag wohl auch die Unkenntnis der technischen Grundlagen sein. Diese Zurückhaltung ist hier aber fehl am Platze, da der E-Commerce die Unternehmer in die Lage versetzt, einen lange gehegten Wunsch zu verwirklichen: Den perfekten Kapitalismus. Das Internet als technische Basis des E-Commerce stellt mittlerweile die notwendige Infrastruktur dafür bereit. Hierauf wird an späterer Stelle noch ausführlich Rücksicht genommen.

1.1 Potential des Electronic Commerce

Die Meinungen darüber, wie groß das Potential des E-Commerce ist, gehen momentan noch stark auseinander, aber ein steiler Aufwärtstrend wird aber von allen führenden amerikanischen Instituten prognostiziert, wie untenstehende Grafik verdeutlicht.



Die Vorhersagen streuen stark durch die Wahl der Methoden [1]

Die Grafik zeigt aber auch, dass vorerst das große Geld nicht im Bereich der Endkunden, sondern im Bereich Business-To-Business, also im Handel zwischen den Unternehmen liegt. Dies ist nicht verwunderlich, denn es spiegelt nur den realen Markt wieder, in dem der Bereich Business-To-Business etwa den zehnfachen Umfang des Endkundenbereiches ausmacht. Aber die Methoden und Verfahren des E-Commerce sind gar nicht so anders als die bisherigen Methoden des Handels. Die weitaus meisten Geschäftsfälle wurden schon immer über große Entfernungen erledigt, entweder per Fax, Telefon, Post oder private elektronische Systeme, wie etwa Mailboxen oder Bulletin Board Systeme. Und die Übertragung dieser Prozesse auf das Internet schafft die Möglichkeit diese billiger, schneller, effizienter und einfacher zu gestalten. Mit welchen Produkten heute bereits gute Umsätze zu erzielen sind, wird durch untenstehendes Diagramm verdeutlicht.

[1] Quelle 3.) S.20

[2]

Es ist daraus auch gut zu erkennen, wie die Eignung der einzelnen Produkte für den Handel im Internet beschaffen ist.

1.2 Kurzer Abriss der Geschichte des Internet

Da das Internet die technische Basis des Electronic Commerce darstellt, soll der Vollständigkeit halber auch ein Abriss über die Geschichte des Internets nicht fehlen.

Das heutige Internet entstand eigentlich aus einem Netzwerk, das für die amerikanische Verteidigung entwickelt wurde. Nach und nach wurde dieses Netzwerk auch zum Austausch von Daten zwischen Wissenschaftlern genutzt und wurde später dann auch für die kommerzielle Nutzung geöffnet. Über die Anfänge des Internets gehen die Meinungen weit auseinander. Dr. Vint Cerf, einer der Väter des Internets, meinte dazu in einem Interview: „Einige Leute legen den Anfang des Internets auf 1969, als der erste Knoten des Arpanet (so der frühere Name des Internets) in den UCLA in Los Angeles eingerichtet wurde. Andere Leute platzieren den Beginn des Internets um 1973, als mein Kollege Bob Kahn die Frage aufgeworfen hat, wie man unterschiedliche Packet-Switching-Netzwerke miteinander verbinden könnte. Wiederum andere sehen den Beginn des Internets im Jahr 1983, als alle Computer des Arpanet von ihren alten Protokollen auf TCP/IP umgestiegen sind. Und für manche hat das Internet erst im Jahr 1994 begonnen, als beinahe jede Zeitschrift und jede Zeitung der Welt fast täglich etwas über das Internet zu berichten wusste, um zu zeigen, dass sie am Puls der neuen Technologien war.“[3] Das Internet selbst ist also nichts Neues. Seit 1969 ist das Netzwerk von den ersten vier Rechnern auf mittlerweile über 5 Millionen Rechner gewachsen und ist damit älter als viele seiner heutigen Nutzer.

Als Urvater des heutige World Wide Web gilt Vannevar Bush, der schon im Jahre 1945(!) in der Zeitschrift The Atlantic Monthly den Artikel "As we may think" veröffentlichte. In diesem Artikel meint Bush, dass es eines der anzustrebenden Ziele sei, Wissen, das weltweit verfügbar ist, allen und jederzeit zugänglich zu machen.

50 Jahre später ist aus diesem Wunsch Realität geworden. Das World Wide Web, ein Internet-Ableger der 90er Jahre, ist eine multimediale Weiterentwicklung der schon bislang im Internet erfolgreichen Systeme wie WAIS und GOPHER.
In Deutschland hat Electronic Commerce eine längere Tradition als viele denken. So wurde bereits 1977 ein öffentlicher Telekommunikationsdienst angekündigt, der die technischen Voraussetzungen schaffen sollte. Dieser Dienst wurde von der damaligen Deutschen Bundespost auf BTX getauft und ist heute allen als t-Online ein Begriff.

[2] Quelle 1.)
[3] Quelle 1.)

2 Technische Aspekte

2.1 Zahlungssysteme

Ein ganz wichtiger und grundlegender Aspekt des Electronic Commerce ist die Bezahlung des Erworbenen, um den elektronisch geschlossenen Vertrag perfekt zu machen.

2.1.1 Klassifizierung der Zahlungssysteme

Grundsätzlich können die elektronischen Zahlungssysteme verschieden klassifiziert werden. Auch die Art der Unterteilung ist auf verschiedenen Wegen möglich. Die Vielfalt der Zahlungssysteme zwingt zu so einer Einteilung in verschiedene Kategorien.

Unterscheiden kann man die Arten von Zahlungssystemen nach:

- dem technologischen Konzept (Kreditkarte, Scheck, Münze),
- der Vertraulichkeit und Anonymität des Transaktionskonzeptes,
- der Effizienz und dem Einsatzgebiet (Kosten, Micro-/Macropayment) und
- der Skalierbarkeit.

Das zugrundeliegende technologische Konzept mit den drei bekannten Varianten Karte, Scheck und Münze, ist wie folgt einteilbar:

- Accountbasierte Konzepte, das sind Schecks und Online-Konten

  Bei diesem Konzept wird der Zahlungsvorgang für das kundeneigene Bankkonto ausgeführt. Dies kann natürlich auch ein virtuelles Kreditkonto beim Händler sein. Diese Konten können, wie beim Online-Banking, mit einem Passwort oder einer PIN, und bei Überweisungen oder sonstigen Manipulationen mit Transaktionsnummern (TAN), bedient werden. Die nötigen Unterlagen für die Nutzung erhält der Nutzer auf einem Weg, der die Rechtsgültigkeit der Übergabe sichert, normalerweise per Einschreiben mit Rückschein. In Bezug auf die Kreditfähigkeit des Händlers können folgende verschiedene Kontenarten für den Kunden eingerichtet werden:

  - *Kreditkonto:* Der Kunde erhält ein Limit, in dem er auf Kredit einkaufen kann. Nach Ablauf eines bestimmten Zeitraums, beispielsweise einen Monat, muss der Kunde das Konto durch eine Überweisung von seinem realen Bankkonto ausgleichen. Wird das Limit überschritten, muss das Konto sofort ausgeglichen werden.
  - *Guthabenkonten:* Hierbei muss der Kunde zuerst einen bestimmten Betrag überweisen, von dem dann Einkäufe getätigt werden. Sobald das Konto erschöpft ist, muss erneut überwiesen werden.
  - *Einzugskonten:* Hier wird nach jeder Transaktion, die das Konto belastet hat, sofort per Einzug vom realen Bankkonto des Kunden der Zahlungsbetrag ausgeglichen. Lieferung und Zahlung erfolgen üblicherweise zeitgleich.

- Inhaberbasierte Verfahren mit Software und elektronischen Münzen

Dieses Verfahren benutzen elektronisches Geld, welches verschiedene Institutionen herausgeben. An späterer Stelle werden einige exemplarisch dargestellt. Hierbei muss der Kunde reales Geld an den entsprechenden Herausgeber schicken, der dieses dann in elektronisches Geld umtauscht und per eMail zustellt. Der Kunde kauft dann Waren, die

elektronischen Münzen gehen in den Besitz des Händlers über, der diese dann wieder in reales Geld umtauscht.

- Inhaberbasierte Verfahren mit Hardware, das sind Kreditkarten und SmartCards

Das ist das am weitesten verbreitete Verfahren und auch vielen bekannt. Darunter fallen Kreditkarten, Geldkarten und SmartCards (z. B. Telefonkarten)

Aus der Art des Zahlungssystems ergibt sich auch das Transaktionskonzept. Einteilbar sind die Transaktionskonzepte nach:

- Anonymen Transaktionen

Bei Verfahren, die auf elektronisches Geld, in größeren Mengen eingetauscht und dann frei und ohne Herkunftsnachweis verteilt basieren, erlaubt dagegen eine gute Anonymisierung. Für Bank und Händler muss sich der Kunde nicht ausweisen oder bekannt machen, die Sicherheit liegt in der Art der Transaktion und der Art des Geldes an sich.

- Nichtanonymen Transaktionen

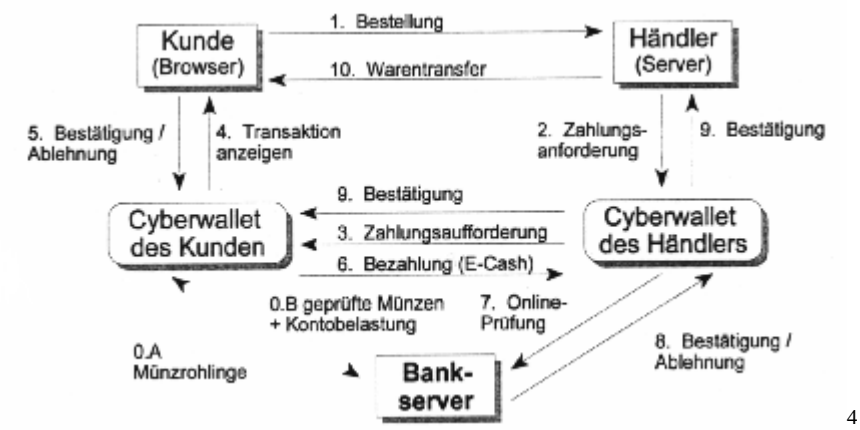
Bei allen Verfahren, die für eine einzelne Bezahlung auf reale Bankkonten zurückgreifen, ist keine Anonymisierung gegeben. Jede Transaktion erscheint auf dem Kontoauszug. Außerdem wird jede Transaktion gespeichert und ist damit nachvollziehbar.

Nach dem Einsatzgebiet unterscheidet man die Zahlungssysteme vor allem durch die pro Transaktion entstandenen Kosten. Drei Bereiche können unterschieden werden:

- Picopayment, für Beträge mit einem Äquivalenzwert von bis zu 10 Pfennigen und Teilungen herab bis zu hunderstel Pfennig. Geeignet für die Bezahlung von Datenabrufe und Informationen sowie Zeiteinheiten.
- Micropayment, für Beträge bis 5 Mark und Teilungen bis zu einem Pfennig. Dieser Bereich deckt alle kleineren Geschäfte ab, wie größere Datenabrufe und Nachrichten.
- Macropayment, für größere Beträge ab 5 DM und Teilungen bis 1 Pfennig. Dieser Bereich ist prädestiniert für Geschäfte bei denen Waren aus der realen Welt gekauft oder verkauft werden.

2.1.2 Elektronisches Geld

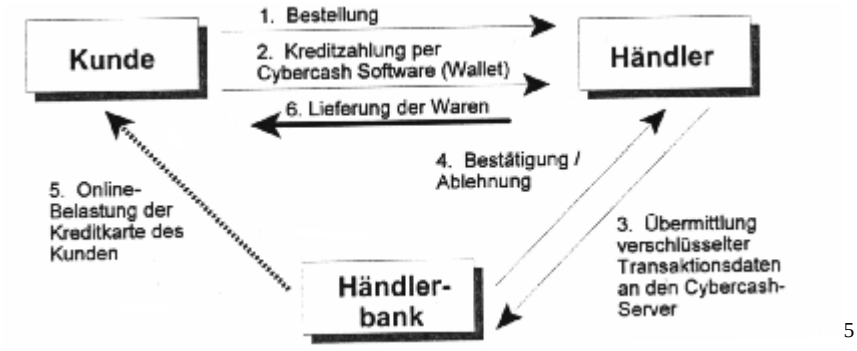
Hier sollen exemplarisch einige Varianten des sogenannten E-Cash vorgestellt und erklärt werden.
Anders als Bargeld oder kartenbasierte Systeme zielt Digicash (http://www.digicash.com) nur auf das Internet und ist damit bestens für Online-Shops geeignet. Digicash verwendet sogenannte Token in Form digitaler Signaturen, die die Nutzer bei ihrer Bank in Geld umwandeln können. Jeder Token kann nur einmal verwendet werden und wird dann zu der ausgebenen Bank zur Prüfung und Inzahlungnahme weitergeleitet. Untenstehende Grafik erläutert das Modell.



4

Das sogenannte Blinding stellt sicher, dass die Identität des Kunden nicht zurückverfolgt werden kann. Beträge sind ab 1 Pfennig möglich und etwa 100 Anbieter weltweit akzeptieren das elektronische Geld bereits.

Das System Cybercoin von Cybercash ist geeignet für Beträge ab 25 Cent bis 10 Dollar. Cybercoin (http://www.cybercash.com) verlangt aus Sicherheitsgründen vom Händler eine Lizenzierung und wird darüber hinaus vom Händler bezahlt. Weltweit akzeptieren 120 Händler das Cybercash-Geld. Cybercash benutzt eine sichere 1024 Bit Verschlüsselung zur Codierung der Transaktionsdaten. Untenstehendes Diagramm erläutert das System detailliert.



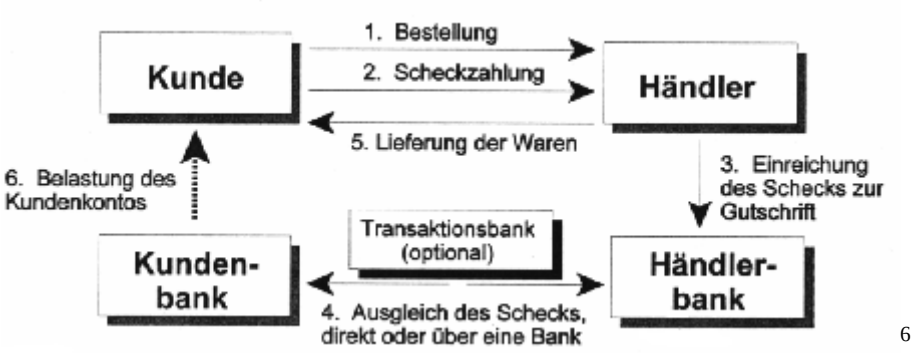
5

Ein wichtiger Vorteil ist die Online-Verifikation der Daten. Die notwendige Software ist für den Kunden bei Cybercash kostenlos erhältlich. Die Bezeichnung Cybercoin ist ebenso wie der Name der Software, "Wallet", irreführend. Cybercoin ist nicht münzbasierend, sondern überträgt nur Kreditkartenangaben auf einem sicheren Weg. Als Geldtauschinstitut dienen Banken, die entsprechende Cybercash-Server betreiben. Der Händler ist somit auf die Zusammenarbeit mit solchen Banken angewiesen.
Ein völlig anderes Prinzip liegt dem Verfahren Netcheque zugrunde. Das von Clifford Neumann an der University of Southern California entwickelte Verfahren überträgt das Prinzip des Verrechnungsschecks auf elektronische Systeme. Der elektronische Netcheque enthält alle Angaben, die auch auf einem normalen Scheck zu finden sind:

- die Kontonummer des Ausstellers
- die Bezeichnung des Empfängers
- den Zahlungsbetrag und die Währung, in der bezahlt werden soll
- eine digitale Unterschrift, die die Echtheit bestätigt

[4] Quelle 3.) S. 91
[5] Quelle 3.) S. 93

Auch Netcheque ist nicht anonym, wie richtige Schecks es auch nicht sind. Vorteilhaft ist die Transportierbarkeit des Schecks. Der Datenblock kann weitergereicht und gespeichert werden. Solche Schecks eignen sich bei entsprechender Sicherheitsstufe der digitalen Signatur vor allem für größere Bezahlungen. Netcheque wird aber leider kaum akzeptiert.



[6]

2.1.3 SmartCards

Einer der attraktivsten und sichersten Methoden elektronischen Geldes, die entwickelt wurden, ist die Smartcardtechnologie (Geldkarten). Das ist eine Karte mit einem Mikrochip, der virtuelles Geld in Form von digitalen Geldeinheiten speichern und abgeben, sowie wieder aufgefüllt werden kann. Der Kauf von Waren und anderen Leistungen kann dann ohne die sichtbare Übergabe von Geld stattfinden. Der wesentliche Vorteil dieses Systems ist die Aufladbarkeit der Karte mit einem Bargeldäquivalent. Das bedeutet, dass bei Diebstahl oder Verlust der Karte die Schädigung des Eigentümers auf den gerade in der Karte gespeicherten Wert begrenzt ist. Im Folgenden sollen nun noch einige solcher SmartCard-Systeme vorgestellt werden.

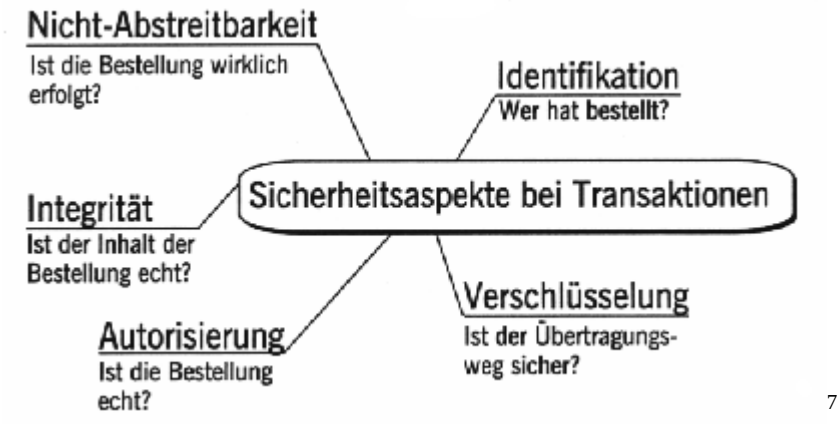
Als Alternative zur Kreditkarte entwickelte die Stuttgarter Telecash (http://www.telecash.de) die TC-Moneybytes. Der Kunde zahlt mit dem Geldkartenchip auf seiner EC-Karte. Für PCs gibt es einen Adapter, der ins Diskettenlaufwerk geschoben wird. Der Betrag wird dann vom Chip abgebucht. Dieses System hat gute Chancen in Deutschland, da hier die EC-Karte sehr verbreitet ist und sie wird eher als Kreditkarten akzeptiert.

Die Fa. Banksys, das belgischen Zahlungsnetzwerk, begann die Vermarktung ihrer SmartCard 1995. Die Karte wird mit Hilfe von Bankautomaten geladen und kann für kleinere Einkäufe bis Bfr 5000,- (ca. 280 DM) genutzt werden. Etwa 32.000 Protonkarten sind im Umlauf und die Transaktionen betrugen 139 Millionen Belgische Franc bis Ende 1995. So wie in Belgien ist Proton auch in der Schweiz, Australien, Brasilien und in den Niederlanden im Einsatz.
Eine interessante Hardwarelösung ist der MeChip, der 1994 von der ESD GmbH (http://www.esd.de) entwickelt wurde. Hier wird eine SmartCard mit dem speziell designten Chip zwischen Tastatur und Computer geschaltet. Der Chip hat rein kryptongrafische Aufgaben, eine Speicherung oder andere Funktionen innerhalb der Transaktion kann er nicht übernehmen. Eine auf dem PC installiere Software empfängt so nur die von der Karte verschlüsselten Daten. Jede an den Kunden ausgegebene Chipkarte ist mit einer einmaligen Signatur ausgestattet. Da Daten außerhalb des Computers verschlüsselt werden, sind Angriffe von Computerviren oder Hackern zwecklos. Als Anwender tritt derzeit nur die Sparda-Bank Hamburg (http://www.sparda-hh.de) auf. Für den Kunden vereinfacht sich Online-Banking etwas, da die Transaktionsnummern (TAN) entfallen.

[6] Quelle 3.) S. 94

2.2 Sicherheit

Von herausragender Bedeutung ist bei allen Transaktionen im Internet der Sicherheitsaspekt, der durch technische Verfahren gewährleistet werden kann.
Um Transaktionen im Internet im großen Stil abwickeln zu können, sind vor allem Sicherheitsmaßnahmen notwendig. Es gibt eine Reihe von Einzelprozessen, die abgesichert werden müssen. Zunächst muss die Identität der Kommunikationspartner sichergestellt werden. Weiterhin wichtig ist, dass die Nachricht nur vom Empfänger gelesen werden kann. Damit beide Partner die Transaktion als rechtsgültig ansehen, muss die Authentizität sichergestellt werden. Die Nicht-Abstreitbarkeit meint, dass keiner der Vertragspartner im nachhinein die Transaktion rückgängig machen oder leugnen kann. Und letztendlich muss auch sichergestellt werden, dass der Inhalt einer Nachricht nicht verändert wurde (Integrität).

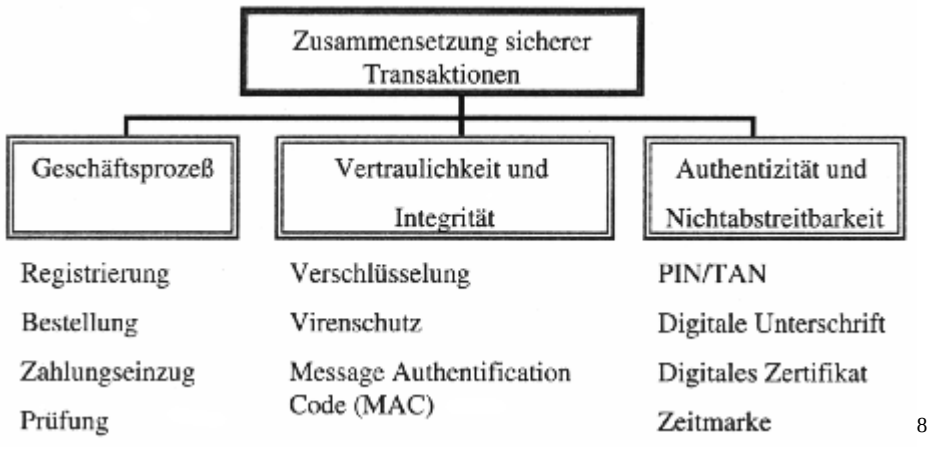


[7]

Elektronische Sicherheit konzentriert sich auf 2 Bereiche:

- Den ungewollten Zugriff auf interne Daten verhindern und
- die Übertragung von Informationen sicherstellen

Sichere Zugriffstechnologien sind für alle Beteiligten von essentieller Wichtigkeit. Sie bilden die Grundvoraussetzungen für den praktischen Betrieb. Einmal unterwegs, kann die Information durch Verschlüsselungstechniken geschützt werden und durch Authentifizierungssoftware kann der Absender festgestellt werden. Beides verhindert, dass nichtautorisierte Personen die Daten manipulieren können.



[8]

[7] Quelle 3.) S.87
[8] Quelle 3.) S.88

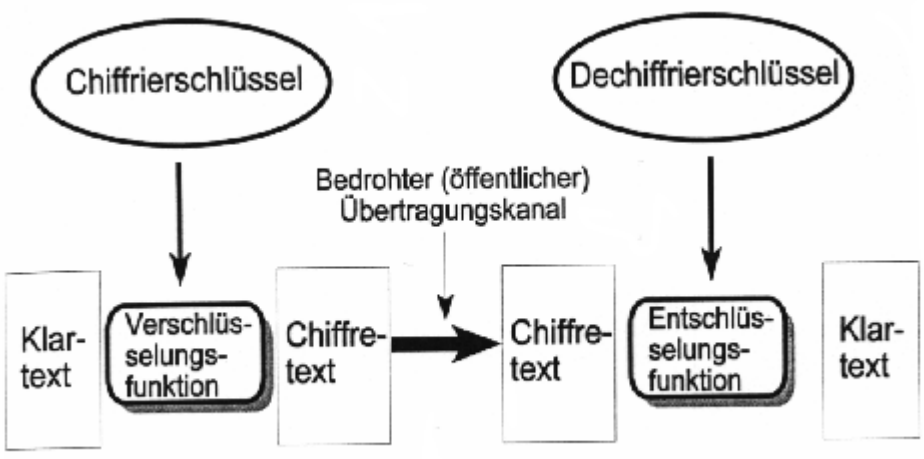
Generell gibt es drei Mechanismen zur Zugangsprüfung:

- Überprüfung von personengebunden Merkmalen (Unterschrift, Fingerabdruck, Gesichtserkennung)
- Inhaberbezogene Kriterien (Besitz einer Kreditkarte, Chipkarte, einer bestimmten Hardware) auf Hardwarebasis
- Inhaberbezogenes Wissen, das sind PIN-Nummer, TAN-Nummern, Passwörter und andere softwarebasierte Verfahren

Eine ganze Anzahl von Zahlungsmethoden sind für den elektronischen Handel entwickelt worden, von denen einige schon an anderer Stelle erläutert wurden. In jedem Fall aber sind es inhaberbezogene Verfahren, denn personengebundene Überprüfungen scheiden durch die Natur des Electronic Commerce aus.

2.2.2 Verschlüsselung

Alle Verschlüsselungsverfahren basieren auf dem gleichen Grundprinzip. Durch die Anwendung einer Schlüsselfunktion auf die zu übertragenden Daten werden die Informationen für den Transport über öffentliche Kanäle unlesbar gemacht. Verschlüsselungssoftware besteht immer aus zwei Teilen, einem beim Server und einen beim Client. Damit wird klar, dass der Einsatz von Verschlüsselungsverfahren bestimmen Standards unterliegen muss, der Betreiber einer elektronischen Handelslösung kann nicht einfach eine für ihn ideale Variante einführen, ohne auf die Belange der potentiellen Kunden einzugehen. Einige Standards und Prinzipien haben sich durchgesetzt, die im folgenden kurz vorgestellt werden sollen.



[9]

Die Verwendung von Verschlüsselungsmethoden für Karten- und Inhaberdetails ist ein zentraler Punkt für den Erfolg der kommerziellen Nutzung des Internets. Im Moment ist das Haupthindernis für die weltweite Akzeptanz der globalen Verschlüsselungsmethoden die US Regierung, die die öffentliche Verschlüsselung mit einem 128-bit Schlüssel als militärische Waffe ansieht und den Export bislang untersagt. Dennoch sieht es so aus, dass dieses Gesetz überarbeitet und entschärft wird, um US Firmen die Belieferung des globalen Marktes zu ermöglichen. Inzwischen ist für Tochterfirmen amerikanischer Konzerne einfach, die Verschlüsselung anzuwenden, ohne damit das Exportverbot zu umgehen. Welche Sicherheit der bislang verwendete 40-bit Schlüssel und der nach mehrfachen erfolgreichen Entschlüsselungsversuchen gerade etablierte 56-bit Schlüssel bietet zeigt die folgende Übersicht[10].

[9] Quelle 3.) S. 99
[10] Quelle 2.) S.124

Angreifer	Budget	Benötigte Zeit für Entschlüsselung 40-bit Schlüssel	56-bit Schlüssel
Jedermann	Minimal	1 Woche	Unmöglich
Kleinunternehmen	$ 400	5 Stunden	38 Jahre
Großunternehmen	$ 10 Mio.	0,005 sec	6 Minuten
Geheimdienst	$ 300 Mio.	0,0002 sec	12 sec

Damit wird klar, dass Geheimdienste gering verschlüsselte Nachrichten theoretisch verzögerungsfrei mitlesen können.

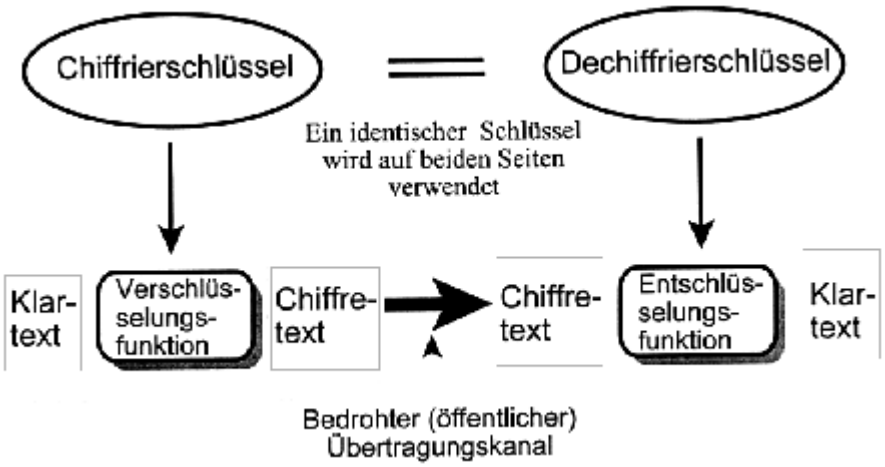
2.2.3 Digitale Unterschriften

Viele Prinzipien der Kryptographie mit verschiedenen Methoden zur Prüfung und Verifizierung der Authentizität von elektronischen Dokumenten, Nachrichten und Transaktionen, verwenden digitale Unterschriften. Der Zweck ist die Authentifizierung sowohl des Absenders als auch der Botschaft selbst, um dem Empfänger die Sicherheit zu geben, dass der Absender wirklich Erzeuger der Nachricht war und dass der Inhalt unterwegs nicht geändert wurde. Digitale Unterschriften sind auch die Grundlage für die Sicherheit mancher SmartCardsysteme. Das Ziel jeder Signatur ist die Beglaubigung einer Nachricht. Also kann eine digitale Unterschrift nicht nur den Absender identifizieren, sondern auch sicherstellen, dass der Inhalt der Nachricht während der Übertragung nicht verfälscht wurde. Eine digitale Unterschrift besteht aus Daten, die auf elektronischen Medien aufgezeichnet werden. Sie wird durch die Anwendung eines mathematischen Algorithmus auf die Nachricht erzeugt - der Signaturfunktion. Die Unterschrift selbst erscheint als zufällige Datenfolge und hat nur eine Bedeutung zusammen mit der Nachricht, aus der sie erzeugt wurde. Der Empfänger der Nachricht prüft die Unterschrift durch die Anwendung eines zweiten Algorithmus auf die gesamte Nachricht - der Prüffunktion. Das positive Ergebnis dieser zweiten Berechnung, authentifiziert sowohl den Absender als auch den Inhalt der Nachricht.

Besser als die Erzeugung immer neuer Signatur- und Prüffunktionen für jeden individuellen Nutzer ist die Verwendung einer allgemeinen Methode mit einer sehr großen Anzahl von Parametern. Die Parameter, sogenannte Schlüssel, erlauben vielen Anwendern, dieselbe Methode zu verwenden, weil sie verschiedene Ergebnisse mit ihren eigenen einmaligen Schlüssel erzeugen. Die zwei am häufigsten angewendeten Methoden für die Erstellung und Prüfung digitaler Unterschriften sind die Methoden Secret-Key und Public-Key.

2.2.3.1 Die Methode "Secret-Key"

Diese Methode verwendet denselben Schlüssel sowohl zur Verschlüsselung als auch zur Entschlüsselung der Botschaft und auch die Signatur- und Prüffunktion sind identisch. Die Daten der Nachricht werden mit der Signaturfunktion durch Verwendung eines Secret-Key-Parameters gekennzeichnet. Die Ausgabe dieser Funktion ist die gesamte Nachricht, die an den Empfänger gesendet wird und anschließend von diesem überprüft wird. Der Empfänger prüft die Unterschrift in der Nachricht durch die Anwendung der Prüffunktion. Diese Funktion verwendet denselben Parameter. Die Ausgabe dieser Funktion ist entweder korrekt oder nicht, je nachdem, ob die Signatur passt.



[11]

Die Secret-Key-Methode beinhaltet aber ein bedeutendes Sicherheitsrisiko. Geräte zur Prüfung der Unterschrift müssen den geheimen Prüfschlüssel kennen. Solche Geräte sind nicht sicher, denn sie können kaum vor ungewolltem Zugriff geschützt werden. Sichere Geräte sind zu teuer und können trotzdem einem Kriminellen nicht standhalten. Dieses Problem schränkt die Nutzung des Verfahrens für Systeme ein, die global eingesetzt werden sollen. Die Methode Public-Key bietet einen Weg zur Lösung des Problems, denn dort müssen die Geräte zur Überprüfung der Nachricht nur einen öffentlich bekannten Schlüssel zur Prüfung haben.

2.2.3.2 Die Methode "Public Key"

Die Public-Key Methode verwendet einen geheimen Schlüssel um die Nachricht zu kennzeichnen. Ein öffentlicher Schlüssel kann aber die Nachricht überprüfen. Der geheime und der öffentliche Schlüssel bilden ein Paar. Der öffentliche Schlüssel kann nur zur Überprüfung verwendet werden und muss deshalb nicht geheimgehalten werden. Die spezielle Ausführung des Schlüssels erlaubt es dem Empfänger, die Echtheit der Nachricht zu überprüfen, aber nicht zu bestimmen, wie die Unterschrift erzeugt wurde. Das bedeutet, dass der öffentliche Schlüssel nicht verwendet werden kann, um Unterschriften zu fälschen oder falsche (fremde) Signaturen zu erzeugen. Eine der bekanntesten Methoden nach diesem Verfahren ist die sogenannte RSA-Methode, das Rivest-Shamir-Adleman Kryptographiesystem, benannt nach den Entwicklern (http://www.rsa.com).

2.2.4 Übertragungsverschlüsselung

Die Kombination von kryptografischen Verfahren führen zu Systemen, die eine sichere Übertragung von Daten über das Internet erlauben. Damit werden elektronische Transaktionen sicher vor Angriffen auf dem Übertragungsweg geschützt. Letztendlich hängt aber die Leistungsfähigkeit aller Verfahren von den verwendeten Schlüssellängen ab. Immer wieder werden Verfahren nach dem "Brute Force"-Methode geknackt. Dabei setzt sich niemand mit der Intelligenz des Verfahrens auseinander, um Schwachstellen zu suchen, sondern es werden einfach alle Kombinationen mit geballter Rechnerkraft ausprobiert. Mit spezieller Hardware kann das auch bei großen Schlüsseln sehr schnell gehen.

[11] Quelle 3.) S. 102

2.2.4.1 Protokolle

Auf der Basis eines 40-bit Schlüssels wurden zwei weitverbreitete Sicherheitsprotokolle entwickelt, die heute weltweit in Browsern verfügbar sind. Für Anwendungen im Internet werden besonders verwendet:

- SSL (Secure Socket Layer)
  SSL wurde von Netscape (http://home.netscape.com/info/scurity-doc.html) entwickelt und hat in ihren weitverbreiteten Browser Netscape Navigator integriert. Durch dessen dominierenden Marktanteil hat SSL eine große Verbreitung gefunden. Beim Verbindungsaufbau authentifiziert sich der Server und optional auch der Client per SSL. Anschließend wird ein Sitzungsschlüssel nach einem asymmetrischen Verfahren ausgetauscht. Der ausgetauschte Schlüssel wird anschließend mit einem symmetrischen Übertragungsverfahren benutzt, vor allem aus Gründen der begrenzten Rechenleistung der Client-Computer. Als Zugriffsprotokoll wird im Namen der URL statt dem bekannten "http:" der Code "https:" benutzt. Damit wird sichergestellt, dass statt des Standardports 80 der dafür reservierte Port 443 im Webserver benutzt wird.
- S-HTTP (Secure HTTP)
  S-HTTP bietet ähnliche Funktionalität wie SSL. Dieses Protokoll wurde von Terisa Systems entwickelt. Die Verbreitung ist allerdings noch relativ gering. Der Vorteil gegenüber SSL ist die Unterstützung der Protokolle auf Anwendungsebene und es kann somit an die gewünschten Sicherheitsanforderungen angepasst werden.

3 Betriebswirtschaftliche Aspekte

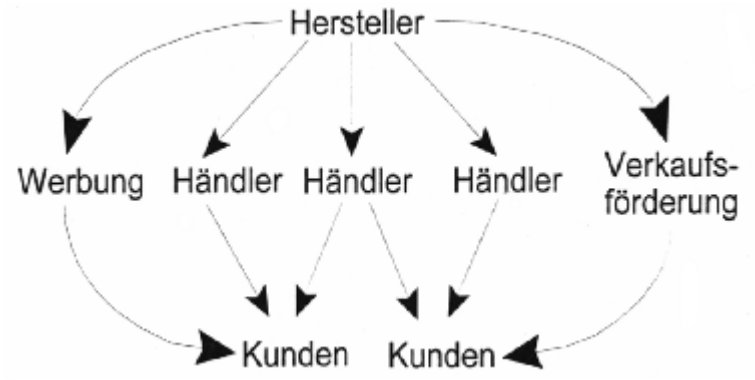
3.1 Geschäftsmodelle

Obwohl erfolgreiche Beispiele von Projekten im Bereich des elektronischen Handels noch dünn gesäht sind, bieten die Erfahrungen der ersten Anwender einen Einblick in Technik und ökonomische Modelle. Es zeigt sich auch, wie ein ganzes Gebiet von wertsteigernden Effekten auftaucht. Das elektronische Handelsmodell vertauscht das herkömmliche "Top-Down"-Modell: "Hersteller-Händler-Konsument", gegen eine "Bottom-Up"-Strategie: "Kunde-Händler-Hersteller". Der Kunde wird zum bestimmenden Faktor, der Anbietermarkt wandelt sich in einen Konsumentenmarkt.

Wo der Kunde tonangebend ist und die Möglichkeit besteht, neue Unternehmen zu niedrigen Kosten aufzubauen, werden viele Geschäfte forciert. Die zukünftige Rolle des elektronischen Handels wird stark aufgewertet. Es wird fundamentale Änderungen in der grundlegenden Kraft der Käufer-Verkäufer-Beziehungen geben.

3.1.1 Das konventionelle Modell

Im konventionellen Handelsmodell nutzen Lieferanten die Kette über etablierte Vermittler - das sind Großhändler, Händler, Agenten - um die Kundenbasis zu erreichen und Service und Unterstützung zu liefern. Riesige Werbekampagnen und Händlerunterstützung erzeugen ein Bewusstsein von Produkten und Service, was den Aktivitäten der Händler hilft.



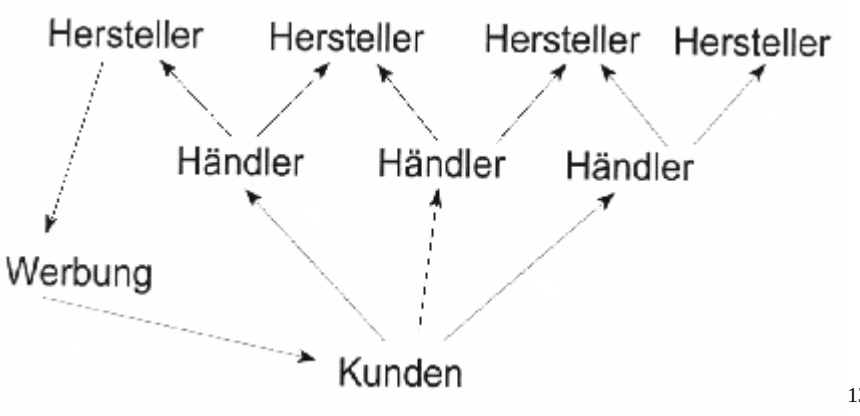
[12]

Im Modell des elektronischen Handels wählt der Kunde einen von vielen Kanälen zu einem Lieferanten, gesteuert durch Preis, sichtbare Eigenschaften und Qualität der Information und des Service. Weiterhin sind Hersteller in einer Position, Produkt und Markenwerbung direkt an den potentiellen Kunden liefern zu müssen, womit viele der Aufwendungen für die Unterstützung der Handelskanäle eingespart werden können, weil der Kunde seine Kaufentscheidung lange vor dem ersten Kontakt mit dem eigentlichen Händler trifft.

3.1.2 Das elektronische Modell

Das bedeutendste Element der neuen Kette ist das Niveau der vom Kunden initiierten Kontrolle, mit der er den Handel in einem größeren Maße beeinflussen kann. Zusätzlich bietet der elektronische Handel viele Vorteile, die in der Natur der Sache liegen, was die positive Erfahrung der Kunden beim Umgang mit dem Medium bestärkt.

[12] Quelle 3.) S.71



[13]

Das elektronische Handelsmodell erlaubt es dem Kunden, die zum Kauf führenden Prozesse stärker zu beeinflussen. Während die Werbung direkt vom Hersteller zum Kunden getragen wird - wie bisher auch - wird andererseits der Händler aus seiner aktiven Vermittlerrolle gedrängt. Der Kunde sucht sich auf elektronischem Wege die den Kauf bestimmenden Faktoren und beauftragt dann den Händler mit der Lieferung. Die Einflussnahme des Händlers auf den Kunden wird reduziert, andererseits wird die Position der Vermittler gegenüber den Herstellern verbessert. Sie sind nicht nur Erfüllungsgehilfen, sondern agieren als Servicecenter der Hersteller.

3.2 Vorteile des Electronic Commerce

Der elektronische Handel bietet einige grundsätzliche Vorteile, die die Käufergunst zunehmend beeinflussen. Diese Vorteile sind so elementar, dass der herkömmliche Handel kaum etwas entgegenzusetzen hat.

Bei neuen Geschäften sollten diese Vorteile gezielt herausgestellt werden, um neue Kunden aktiv zu gewinnen. Folgende Vorteile sind erkennbar:

- Bequemlichkeit: Bei der Auswahl von Produkten und Dienstleistungen kann der Kunde Zeit und Ort entscheiden. Ladenschluss und Fahrstrecke werden irrelevant.
- Schnelligkeit: Der Prozess der Auswahl der Produkte und des Kaufens ist schneller, mehr Produkte können in kürzerer Zeit verglichen werden.
- Information: Die Daten zum Produkt können direkt in den Auswahlprozess integriert werden. Die Kompetenz elektronischer Verkäufer kann deutlich über dem Niveau herkömmlicher Anbieter liegen.
- Unterhaltung: Die Kauferfahrung macht Spaß und bindet stärker an den Händler. "Surfen" ist zum Freizeiterlebnis geworden.
- Kosteneinsparung: 15%-90% des Listenpreises sind für die Bedürfnisse des Handelskanals nötig. Ohne den Handel kann der Preis reduziert werden.
- Personalisierung: Ein persönlicherer Service wird nach den individuellen Bedürfnissen des Kunden möglich. Es kommt quasi einer Automation des Außendienstes gleich.

3.3 Ende des Zwischenhandels?

Ein Prozess ist die Trennung der Vermittler - der Zwischenhändler - von den existierenden Warenketten. Aber damit ist nicht notwendigerweise gemeint, dass dieses Geschäft verschwindet oder dass Arbeitsplätze wegfallen. Die Änderungen an den Stationen, wo

[13] Quelle3.) S.72

Waren und Leistungen vom Hersteller zum Kunden gebracht werden, sind vor allem Änderungen in der Art und Weise, wie Händler arbeiten. Es sind auf diesem Weg eine Vielzahl von Transaktionen abzuwickeln, die weiterhin verschiedene Typen von Händlern benötigen. Einige dieser Typen sind neu und bieten hervorragende Chancen für Jungunternehmer.

Die Ausdehnung des Geschäftes auf den elektronischen Handel erlaubt es dem einzelnen Konsumenten, in Aktienmärkte zu investieren, Güter und Leistungen zu kaufen, überall nach Häusern oder Autos zu suchen, und das alles mit einem Mausklick. Die Abtrennung des Zwischenhandels bringt die Wertschöpfung. Es erfolgt ein Umstieg von existierenden Medien auf neue und keine einfache Beseitigung der ganzen Handelskette. Die Vermittler und Makler können sich mehr auf die Verteilung von Produktinformationen konzentrieren und agieren als Handelsvertreter. Börsenmakler werden weiter gebraucht, um für Aktienkäufe zu werben und Tipps zu geben. Einzelhändler werden Produktdaten liefern und Werbung für Produkte machen, sicher in größerem Umfang und in anderer Form als heute. Händler und Makler werden trotzdem benötigt, um Garantieleistungen und Service für hochwertige Güter im Namen der Hersteller zu erbringen. Es wird ein starkes Wachstum geben in der Entwicklung von Software für den elektronischen Handel und für die Schulung, Information und Verwendung der Software, auch das sind neue Chancen für etablierte Händler.

In diesem Licht betrachtet kann die Beseitigung des Zwischenhandels als Wertsteigerung wahrgenommen werden. Neue Medien bringen neue Firmen in die Wertkette. Die Beseitigung des Zwischenhandels demonstriert die Fähigkeit, Werte auf alternative Liefermechanismen zu übertragen, anstatt einfach nur den Handel zu eliminieren. So wie neue Kanäle am Markt entstehen, können sich Firmen mit hoher Flexibilität in der Organisation Vorteile schaffen, trotz der Bedrohung des Zwischenhandels. Firmen die weniger funktionell organisiert sind können neue Marktmöglichkeiten eher erkennen und umsetzen. Diese Firmen werden die Technologie benutzen, um die neuen Geschäftsprozesse zu beschleunigen. Grundsätzlich werden Begrenzungen des herkömmlichen Geschäftes überwunden. Die Firmen werden innovativer bei der Gewinnung neuer und der Pflege existierender Kunden. Es gibt eine Menge Geschäftsgebiete, in denen die Beseitigung des Zwischenhandels beginnt. Damit wird die Industrie angespornt, neue Möglichkeiten des Marktes zu suchen und die existierenden Industriemodelle zu ändern.

4 Rechtliche Aspekte

Die bisher gemachten Aussagen über den E-Commerce zeigen ihn als durchaus interessantes und lukratives Geschäftssystem. Wie sieht aber der rechtliche Rahmen für solche Geschäfte über das Internet aus? Im weiteren möchte ich nun auf die den Zahlungsvorgängen zugrundeliegenden Verträge eingehen und inwieweit sie von deutschen Gerichten anerkannt werden.

4.1 Vertragliche Vereinbarungen

Verträge sind die Grundlage eines jeden rechtsverbindlichen Geschäftes. Deshalb vorab einige Informationen über Verträge grundsätzlich und danach noch einige Aspekte, die im Bereich E-Commerce relevant sind.

4.1.1 Formfreiheit

Das BGB setzt für das Zustandekommen eines rechtsgültigen Vertrages grundsätzlich zwei inhaltlich übereinstimmende Willenserklärungen voraus. Dies ist auch bei elektronisch geschlossenen Verträgen ohne Schwierigkeiten zu erfüllen. Juristen sehen dies ebenso und stehen deswegen Verträgen die per eMail oder sonstigen elektronischen Medien zustande kommen keineswegs ablehnend gegenüber. Sie erachten diese Willenserklärungen für rechtsverbindlich, genau so wie Erklärungen, die mündlich oder schriftlich erfolgt sind. Dies erklärt sich dadurch, dass der Gesetzgeber bis auf einige Ausnahmen (z. B. bei Kauf oder Verkauf von Grundstücken) für Vertrage keine bestimmte Form zwingend vorschreibt. Demnach könnten Verträge mündlich, über ein elektronisches System oder sogar stillschweigend geschlossen werden. Zu Verträgen, die über ein solches elektronisches System zustandekamen gibt es auch schon einige Urteile deutscher Gerichte, die man exemplarisch anführen kann. Beispielsweise im Zusammenhang mit dem früheren BTX-Angebot der Deutschen Post AG. Deutsche Gerichte haben mehrfach Verträge anerkannt, die dadurch zustandekamen, dass ein Käufer auf einer BTX-Angebotsseite seinen Willen zum Kauf durch die Eingabe der Zahlenkombination 19 kundtut und der entsprechende Anbieter durch die Übersendung der Ware den Kaufvertrag vervollständigt.

4.1.2 Urkunden

Aber nicht immer geht das so einfach. Dies gilt insbesondere für Verträge die der Schriftform bedürfen. Dann benötigt man zum Zustandekommen eines Vertrages nach §126, Abs. 1 BGB eine Urkunde, die vom Aussteller eigenhändig unterzeichnet wurde. Elektronische Dokumente auf der Festplatte des Computers sind nach der Ansicht der überwiegenden Zahl der Richter, die sich hiermit befasst haben, keine Schriftstücke, die dieser Form genügen. Die Argumentation geht hier den Weg, dass eine Urkunde direkt gelesen werden kann, ein elektronisches Dokument hingegen erst lesbar gemacht werden muss. Man geht sogar so weit, dass man sagt, das die Visualisierung auf dem Monitor oder der Computerausdruck nur das Abbild des gespeicherten Dokuments seien.

4.1.3 Rechtssicherheit

Rechtssicherheit ist momentan bei Geschäften übers Internet noch nicht voll gegeben, da einige Detailfragen beim Online-Vertragsschluss noch nicht endgültig geklärt sind. Wer dieses Risiko scheut kann aber dennoch vom E-Commerce profitieren. Viele Unternehmen

nutzen Ihre Web-Sites in erster Linie als Präsentationsplattform für ihre Produkte und erst in zweiter Linie um Umsatz zu generieren. Genau dies kann sich der Kunde zunutze machen.
Er informiert sich im Internet über das Produkt und kann mit Hilfe von Online-Shops einen Preisvergleich durchführen. Danach kann er wie bisher bei einem Händler sein Produkt kaufen und umgeht somit das Risiko der nicht vollständig gewährleisteten Rechtssicherheit. Bei Verträgen mit niedrigem Transaktionsvolumen kann man dieses Risiko aber ziemlich vernachlässigen.

4.2 Rahmenverträge und AGB

Um aber in absehbarer Zeit doch die Rechtssicherheit und Rechtsverbindlichkeit voll herstellen zu können sind Rahmenverträge und AGB das adäquate Mittel. Als Beispiel für diese Rahmenverträge stehen die EDI-Protokolle.

4.2.1 EDI

Bereits im Januar 1994 hat die damalige EG-Kommission eine Empfehlung zu den rechtlichen Aspekten des Electronic Data Interchange (EDI) veröffentlicht. Hauptziel dieser Empfehlung war die Erhöhung der Wettbewerbsfähigkeit besonders von kleinen und mittleren Unternehmen, dadurch dass ihnen durch diese Empfehlung der Aufwand für eine eigene Vertragsgestaltung erspart wird.

Es existiert bereits ein deutscher EDI-Modellvertrag, der u. a. Regelungen zu den vertraglichen Beziehungen zwischen EDI-Partnern enthält. Geregelt werden darin u. a.

- der Zugang einer Nachricht
- die Haftung für fehlerhafte Übermittlung
- der Beweiswert von EDI-Dokumenten
- der Datenschutz bei der Elektronischen Nachrichtenübermittlung

Man sieht also deutlich die Ansätze der Politik, den Electronic Commerce durch entsprechende Rahmenverträge zu formalisieren.

4.2.2 Formalisierung des E-Commerce durch Rahmenverträge

Solche Rahmenverträge sind eine sinnvolle Alternative für alle, die sich auf rechtlich eher sicherem Gebiet bewegen möchten. Man formuliert am besten auf der Grundlage der genannten EDI-Empfehlung einen solchen Rahmenvertrag und lässt diesen am besten von einem kompetenten Rechtsanwalt prüfen. Bei der Formulierung ist aber folgendes zu beachten:

- Rahmenverträge sind nur dann wirksam, wenn von beiden Vertragsparteien die Geltung ausdrücklich vereinbart worden ist
- Es sollte überprüft werden, ob die technischen Regelungen des EDI-Protokolls nicht in Teilbereichen schon wieder überholt sind, da sich in diesem Bereich die Rechtsprechung in nächster Zeit sehr schnell entwickeln wird
- Vereinbarungen hinsichtlich elektronischer Nachrichten sind nur dann sinnvoll, wenn diese elektronisch signiert werden. Nur dann ergibt sich eine gewisse Gewähr dafür, dass die eMail auf dem Weg zum Empfänger nicht von Unbefugten geändert wurde.

Wie verhält es sich nun aber mit den obengenannten Allgemeinen Geschäftsbedingungen (AGB) im Bereich des Electronic Commerce?

Mit AGB als vorformulierte Vertragsbedingungen arbeiten heute in der BRD fast alle Kaufleute. Sie bieten den Vorteil, dass nicht bei jedem Vertragsschluss wichtige Absprachen wie Zahlungsmodalitäten, Gerichtsstand, Gewährleistungsansprüche und anwendbares Recht nicht jedes mal individuell vereinbart werden müssen. Sie gelten per AGB in gleicher Weise für eine unbestimmte Anzahl von Verträgen mit verschiedenen Vertragspartnern.

4.2.3 AGB und Electronic Commerce

Es scheint also ganz einfach zu sein über AGB einen rechtlich sicheren Rahmen für Geschäfte über das Internet herzustellen. Man zeigt dem Kunden vor Vertragsschluss einfach kurz seine AGB und sie sind hiermit rechtskräftig. Doch ganz so einfach ist es doch wieder nicht. Die Klausel, dass die Bedingungen dem Kunden spätestens vor Vertragsabschluß vorgelegt werden müssen, kann damit gerade noch erfüllt werden. Aber §1, Abs. 1 AGBG verlangt zusätzlich bei Nichtkaufleuten, dass der Klauselanwender seinem Gegenüber die Möglichkeit bieten muss, von diesen Klauseln ausreichend Kenntnis zu nehmen. Bei Verträgen zwischen Kaufleuten gestaltet sich dies wesentlich einfacher. Es genügt meistens, dass eine längere Geschäftsbeziehung besteht, denn nach §24 AGBG gelten die engen Einbeziehungsvoraussetzungen aus §2 AGBG bei Kaufleuten nicht, da vorausgesetzt wird, dass sie wissen, dass Verträgen üblicherweise AGB zugrundegelegt werden. Um nun aber auch die strengen Einbeziehungsvoraussetzungen aus §2 AGBG zu erfüllen, wie dies bei Verträgen mit Nichtkaufleuten der Fall ist, muss bei einem Online-Shop eine klar gekennzeichnete Schaltfläche vorhanden sein, die eine Einsicht in die AGB zulässt.

4.3 Rechtsgültigkeit und Zugang von eMails

Ein zentrales Verfahren beim E-Commerce ist die Kommunikation via eMail. Hierbei ergeben sich einige Fragen, die der Klärung bedürfen. Basis für mögliche gerichtliche Entscheidungen ist der Eingang von Willenserklärungen, in diesem Fall Willenserklärungen per eMail, beim Empfänger. Jetzt stellt sich nur die Frage, wann man davon sprechen kann, dass eine eMail beim Empfänger angekommen ist. Etwa nach Absendung des Senders, bei Eingang der eMail auf dem POP3-Konto des Empfängers oder gar erst wenn dieser sein eMail-Account abruft? Und wer soll beim Abruf das Übermittlungsrisiko tragen, wenn aus technischen Gründen Emails verloren gehen?
In §130 Abs. 1 BGB definiert die Rechtsprechung, dass Angebot und Annahme den jeweils anderen Vertragspartner natürlich erreichen müssen, wenn ein Vertragsschluss erfolgen soll. Bei eMail spricht der Gesetzgeber aber von Erklärungen unter Abwesenden und diese werden erst mit dem Zugang beim Empfänger wirksam, also erst wenn der Empfänger diese liest. Bei einem herkömmlichen Schreiben per Briefpost gilt eine Erklärung als zugegangen, wenn sie derart in den Einflussbereich des Empfängers gelangt ist, dass dieser jederzeit darauf zugreifen und der Absender mit einer Kenntnisnahme rechnen kann. Dies ist z. B. der Fall, wenn der Briefträger einen Brief in den Hausbriefkasten wirft. Hier werden dann die üblichen Leerungszeiten unterstellt.
Das OLG Köln hat bereit 1989 entschieden, dass ein Telex, das über Bildschirmtext der damaligen Deutschen Bundespost versandt wurde, in dem Moment als zugegangen gilt, in dem es vom Empfänger im BTX-Postfach abgerufen werden kann. Außerdem hat sich in der Rechtsprechung die Meinung gebildet, dass ein Vertragspartner, der seine eMail-Adresse ausdrücklich als geschäftliche Korrespondenzadresse genannt hat, so zu behandeln ist, wie derjenige der seine Postadresse nennt. An diese Anschrift adressierte und dort eingegangene

Nachrichten gehen in dem Zeitpunkt zu, in dem mit einer Leerung des Postfaches zu rechnen ist. Dies bedeutet im Umkehrschluss, dass ein eMail-Account, das für geschäftliche Zwecke genutzt wird, tunlichst täglich – vorzugsweise vormittags – abgefragt werden sollte. Übermittlungsfehler, die nachweislich auf einem Fehlverhalten des Providers des Empfängers zurückzuführen sind, hat dennoch ausschließlich der Empfänger zu vertreten, denn schließlich hat dieser selbst den Provider eigenständig ausgewählt. Er hat im Falle der Fehlübermittlung zwischen dem Server des Providers und seinem Mail-Client dann bestenfalls noch die Möglichkeit, Regressansprüche für den möglichen erlittenen Schaden zu erheben.
Diese teilweise doch sehr wage Rechtslage wird sich bald ändern. Denn zur Zeit wird in Berlin an einem Signaturgesetz (SigG) gearbeitet, das Bestandteil des Informations- und Kommunikationsdiensts-Gesetzes (IuKDG) werden soll.

„Eine digitale Signatur ist demnach „ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels [...] den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.“ Der Gesetzgeber bezieht sich hierbei auf asymmetrische Verschlüsselungsverfahren.

Instanzen des Signaturgesetzes:

- Der Entwurf zum Signaturgesetz sieht in §2 Abs. 4 SigG als zusätzliches Merkmal einen Zeitstempel vor, mit dem nachgewiesen werden kann, dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben
- Um sicherzustellen, dass ein bestimmter öffentlicher Schlüssel auch einer bestimmten natürlichen oder juristischen Person zugeordnet werden kann, sollen von unabhängigen Zertifizierungsstellen auf fünf Jahre gültige Zertifikate vergeben werden, in denen die Zuordnung bescheinigt wird (§4 SigG). Die Betreiber einer solchen Zertifizierungsstelle müssen zuvor bei der vom Telekommunikationsgesetz (TKG) vorgesehenen Regulierungsbehörde eine Lizenz beantragen. Diese Lizenz wird nach §3SigG ausgestellt, wenn die Zertifizierungsstelle als ausreichend sicher erachtet wird. Ein Beispiel für eine solche Zertifizierungsstelle ist das amerikanische Unternehmen Verisign.
- Hinsichtlich des BGB wird die Verabschiedung des §126a von Bedeutung sein. In diesem Paragraphen wird die sogenannte "Textform" definiert. Mit der Textform wird dann eine Sonderform der schriftlichen Form beschrieben, welche sich gemäß des Gesetzestextes aus Schriftzeichen und Erkennbarkeit der erklärenden Person zusammensetzt. Die Textform ist rein rechtlich weniger mächtig als die Schriftform, welche jedoch in Zusammenhang mit der Änderung des §127 BGB dazu führt, dass eine Wahlfreiheit zwischen Textform und Schriftform möglich wird: „Ist durch ein Rechtsgeschäft bestimmt, dass eine Erklärung schriftlich abzugeben ist, so ist im Zweifel anzunehmen, dass die Einhaltung der für die Textform geltenden Bestimmungen des §126a die Form, wahrt.“

Durch die Verabschiedung des Signaturgesetzes und die Änderung des BGB werden eMails, die mit einem zugelassenen Schlüssel unterzeichnet bzw. signiert wurden rechtskräftig. Dennoch bleibt offen, ob der Gesetzgeber digitale Dokumente in absehbarer Zeit in den Urkundenbegriff integriert. Außerdem ist unklar, ob auch staatliche Gerichte die Beweiskraft von eMail überhaupt anerkennen müssen. Das LG Köln etwa hält Beweiskraftklauseln generell für unzulässig. Aber dennoch können Vereinbarungen, die sich auf signierte eMails beziehen, im Rechtsstreit wichtige Entscheidungshilfen für den Richter darstellen.

Mit elektronischen Vereinbarungen via eMail tun sich deutsche Gerichte generell noch schwer. Fast schizophren erscheint im Gegensatz dazu die geltende Rechtsauffassung bei elektronischen Erklärungen, die innerhalb von geschlossenen Online-Systemen, wie etwa t-Online, abgegeben werden. Ihnen wird eher vertraut als denen, die in eMails abgegeben wurden. Die Gerichte unterstellen hierbei, dass die Erklärung entweder vom Anschlussinhaber selbst oder einem von ihm autorisiertem Benutzer abgegeben wurde. In beiden Fällen sei die Willenserklärung dem Anschlussinhaber zuzuordnen, entweder unmittelbar oder über Vollmachtsbestände. Voraussetzung sei nur, dass bei der Anmeldung nachweislich die Anschlusskennung und das persönliche Passwort benutzt wurden. Ob dieses große Vertrauen in die sogenannten "geschlossenen Systeme" gerechtfertigt ist, darf auf dem Hintergrund des Skandals bei t-Online, bei dem ein Jugendlicher ohne besondere Ausrüstung durch die Änderung von zwei Byte des Codes der t-Online Zugangssoftware alle Passwörter ausspionieren konnte, stark in Frage gestellt werden.“[14]

4.4 Zahlungsvorgänge im Internet

Das gängigste Zahlungsmittel im Internet ist momentan die Kreditkarte. Überweisungen oder Schecks sind eher unüblich. Mit jeder Übermittlung der Kreditkartendaten ist allerdings auch das Risiko des Missbrauchs gegeben. Hacker können Passwörter und Kreditkartennummer abfangen und diese zu ihren eigenen Nutzen einsetzen.
Interessant sind hier nur die Verfahrensweisen mit dem Medium Kreditkarte. Die Bedingungen der Kreditkartenunternehmen gingen bisher davon aus, dass bei Zahlungsvorgängen mit Kreditkarten vom Kunden ein Beleg unterschrieben wird, auf den das Vertragsunternehmen zuvor die Kartendaten übertragen hat, oder dass an Geldautomaten oder automatisierten Kassen vom Kunden die PIN eingegeben wird. Die Realität sieht heute aber völlig anders aus: Es reichen bei vielen Online-Geschäften die Eingabe der Kreditkartennummer und des Verfallsdatums für die Legitimation der Kartennutzung. Wollen wir nur hoffen, dass sich die Kellner in Restaurants, in denen wir per Kreditkarte unsere Rechnung bezahlen, nicht diese Daten schnell notieren und dann – während wir noch am Tisch sitzen – im Internet damit einkaufen gehen.
Wer haftet dann eigentlich? Solange die Karte vom Kunden sorgfältig aufbewahrt wird, so dass sie nicht in die Hände Unbefugter gelangen kann, haftete er bisher nicht für Verbindlichkeiten, die beleglos und ohne Geheimzahl mit der Karte eingegangen wurden. Erfolgt der Karteneinsatz unter Verwendung der PIN beleg- oder unterschriftslos, kann der Karteninhaber die Belastung seines Kartenkontos nur beanstanden, indem er nachweist, dass die Karte nicht von ihm benutzt wurde. Manche AGB von Kreditkartenunternehmen sehen inzwischen zwar vor, dass zwischen Karteninhaber und Vertragsunternehmen ausnahmsweise darauf verzichtet werden kann einen Beleg zu unterschreiben. Eine Verpflichtung zur Übernahme der dem Vertragsunternehmen gezahlten Beträge trifft den Karteninhaber aber trotzdem nur dann, wenn das Kreditkarteninstitut ihm nachweisen kann, dass die Kartennummer von ihm zu Zahlungszwecken weitergegeben wurde. Die Kreditkartenunternehmen gehen sogar so weit, dass bei fehlender Unterschrift die Bestellung auf Wunsch des Kunden storniert werden kann.

4.5 Internationale Aspekte

Die bisherigen Aspekte berührten bisher fast nur die Rechtslage in Deutschland. Deswegen nun noch einen kleinen Ausblick auf internationale Aspekte der Rechtslage.

[14] Quelle 2.) S.107ff

4.5.1 Globales Internet

Das Internet ist keine deutsche Erfindung, erst recht sind die Nutzungsmöglichkeiten des Internets nicht auf den deutschen Rechtsraum beschränkt. Als Beispiel einer solchen Berührung mit anderen Rechtssystemen stellen wir uns einfach einmal den Fall vor, dass Sie auf der Web-Site eines Factory Outlet in den Vereinigten Staaten günstig Turnschuhe eines Markenherstellers bestellen. Hier stellt sich dann die Frage, welche Rechtsordnung ggf. über Zahlungsansprüche und Erfüllungswirkung entscheiden soll.

4.5.2 Internationale Abkommen

Es ist bei solchen Sachverhalten mit Auslandsberührung, die im Juristendeutsch auch als "Kollisionsfalle" bezeichnet werden, zunächst zu prüfen, ob es einschlägige internationale Abkommen gibt. In Betracht kommen neben binationalen Verträgen auch Vereinbarungen, die für eine Vielzahl von Ländern gelten. Beim internationalen Wareneinkauf ist dabei vor allem an das UN-Übereinkommen aus dem Jahre 1980 zu denken. Es hat in vielen Ländern, so z. B. den USA, Weißrussland und in den meisten Mitgliedsländern der Europäischen Union, weitgehend gleichlautende Regelungen geschaffen. Dies allerdings nur in wichtigen Teilbereichen.

4.5.3 Privatrecht

Wenn es diese internationalen Abkommen nicht gibt, muss der Richter sein eigenes Internationales Privatrecht (IPR) danach befragen, welches nationale Recht Anwendung findet. In Deutschland finden sich Vorschriften zum IPR vor allem im Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB). Der Artikel 27 EGBGB sieht hierbei vor, dass die Vertragsparteien grundsätzlich selbst frei wählen können, welchem Recht sie ihr Vertragsverhältnis unterstellen. Die Geltung einer ausländischen Rechtsordnung kann grundsätzlich in den AGB vereinbart werden. Dabei muss man lediglich darauf achten, dass diese Bedingungen auch Vertragsbestandteil, also wirksam mit in den Vertrag einbezogen werden.
Nun denkt sich sicherlich jeder Betreiber eines Online-Shops, dass er eine für sich günstige Rechtsordnung auswählen kann und diese einfach per AGB zur Grundlage aller Verträge macht. Doch ganz so einfach ist es dann doch nicht. Ein Klauselanwender kann sich durch die Wahl seiner eigenen Rechtsordnung nicht zwingend Verbraucherschutzregeln entziehen, die z. B. in Deutschland gelten. Das Gesetz zur Regelung der Allgemeinen Geschäftsbedingungen (AGBG) erklärt sich nämlich selbst dann für anwendbar, wenn ein deutscher Verbraucher in Deutschland umworben wird, und daraufhin einen Vertrag schließt. In diesem Fall sind die Vorschriften des Verbraucherschutzgesetzes nach §12 AGBG trotz der Unterstellung des Vertrages unter ausländisches Recht zu berücksichtigen.

4.5.4 Heimatrecht

Falls im Vertrag nichts über die Unterstellung des Vertrages unter eine bestimmte Rechtsordnung vereinbart ist, so wird ein deutscher Richter im Streitfall nach Artikel 28 EGBGB verfahren. Dort ist festgelegt, dass in einem solchen Fall das Heimatrecht desjenigen Vertragspartners anzuwenden ist, der die Leistung erbringen soll. Das ist im Falle eines Online-Shops in aller Regel der Betreiber.

Qellenverzeichnis:

1.) Microsoft; The Economist

2.) Fochler, Klaus; Perc, Primoz; Ungermann, Jörg: Electronic Commerce mit Lotus Domino;
Addison Wesley Longman Verlag, 1997
S. 107ff, 124, 125, 158, 139ff, 168ff

3.) Krause, Jörg: Electronic Commerce: Geschäftsfelder der Zukunft heute nutzen;
Carl Hanser Verlag Wien, 1998
S. 78, 82ff, 188, 194f

Literaturverzeichnis

Krause, Jörg: Electronic Commerce: Geschäftsfelder der Zukunft heute nutzen; Carl Hanser Verlag Wien, 1998

Fochler, Klaus; Perc, Primoz; Ungermann, Jörg: Electronic Commerce mit Lotus Domino; Addison Wesley Longman Verlag, 1997

Microsoft; The Economist

Riesenkampff, Philipp, Rechtsprobleme des Internet

Rischbode, Horst, Geschichte des Internets,
http://www.users.comcity.de/~horibo/history.htm , Kiel, 1998

Jäger, Markus und Knotzer, Martin, Verbreitungsgrad und typische Einsatzzwecke des World Wide Web,
http://www.ifs.univie.ac.at/~b9200491/verbreitung/geschichte.html , Wien, o.J.

Musch, Jochen, Die Geschichte des Netzes: ein historischer Abriß,
http://www.psychologie.uni-bonn.de/sozial/staff/musch/history.htm#9 , Göttingen, 1997

Juliane G. und Cecile S., Die Geschichte des Internet,
http://www.garf.de/gym-schiff/kurzv/geschich/index4.htm , Karlsruhe, o.J.

Dokters, Stefan, Haftung für Hyperlinks,
http://www.web-kanzlei.de , Münster, 1998

Von Gravenreuth, Günther, Frhr, Gerichtsentscheidungen zum Internet, Strafrechtsfälle,
http://www.gravenreuth.de/strafr.html , München, 1996

Bechthold, Stefan, Multimedia und das Urheberrecht
http://www.jura.uni-tuebingen.de/~s-bes1/sem97/sem.html , Tübingen, 1997

Prof. Dr. Thomas Hoeren, Rechtsfragen des Internet,
http://www.uni-muenster.de/Jura.itm/hoeren/matintrecht/SkriptIR.doc , Münster, 1998

Gerling, Rainer, Internet: juristische Probleme und kein Ende?,
http://www.dfn.de/dfn/erklaerungen/jur-problem_ToC.html , München, 1997

Suchmaschinen:

http://www.infoseek.de

http://www.yahoo.de

http://www.wer-weiss-was.de

*** im Text verwendete Links

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel verwendet habe. Insbesondere versichere ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht habe.

_____

(…)