

Eine Einführung in die Geschäftsmodelle, Anwendungen und Technologien des

Electronic Commerce

Michael Merz

Letzte Aktualisierung: 12.04.99

Inhalt

1 PROLOG IM JAHRE 2025	2
2 WAS IST ELECTRONIC COMMERCE?	8
2.1 Einführung.....	8
2.2 Klassifikationen	9
2.2.1 Akteure und Rollen beim Internet-Handel	9
2.2.1.1 Business-to-Business	10
2.2.1.2 Business-to-Consumer	10
2.2.1.3 Administration-to-Business	11
2.2.1.4 Administration-to-Consumer	11
2.2.1.5 Administration-to-Administration	11
2.2.1.6 Consumer-to-Consumer	11
2.2.1.7 Zusammenfassung	12
2.2.2 Phasen der Handelstransaktion	12
2.2.3 Transaktionsvolumen	13
2.2.4 Anwendungsnähe der EC-Technologie	14
3 ELECTRONIC COMMERCE UND DIE STATISTIK	16
3.1.1 Demographisches aus der Internet-Gemeinde	17
3.1.2 Branchen	24
3.1.3 Informationstechnologie und Medien	26
4 ELECTRONIC COMMERCE IN DER VOLKSWIRTSCHAFT	27
4.1 Rechtliche Rahmenbedingungen.....	27
4.1.1 Vertragsrecht und Internet	27
4.1.2 Das Signatur-Gesetz	28
4.1.3 Die Rolle der Europäischen Kommission	29
4.2 Neue ökonomische Modelle	31
4.2.1 Klassische und neue volkswirtschaftliche Modelle	33
4.2.2 The Winner takes it all... ..	39
4.2.3 Vertrauensökonomie	40
4.2.4 „Vollkasko-Wirtschaft“ vs. „Free-Economy“	41
4.2.5 Netzwerkexternalitäten	42
4.2.6 Free Economy: Kein Umsatz ohne „Teaser“	43
4.2.7 Aufmerksamkeitsökonomie	44
4.2.8 Disintermediation: Vom Händler zum Makler	45
4.2.9 Commoditization	46
4.2.10 Virtual Communities	46
4.2.11 Coopetition	47
4.2.12 Geistiges Eigentum	47
4.2.13 Individualisierung	49
4.2.14 Mikrofinanzierung oder 10 * kleines Risiko < 1 * großes Risiko	49
4.2.15 Elektronische Märkte.....	50
4.2.16 Das Gesetz des einzigen Preises	50
4.3 Die Rolle des Staates	51
4.3.1 Notenbanken in einer bargeldlosen Wirtschaft	52
4.3.2 Zoll und Steuern	53
4.4 Gewinner und Verlierer beim EC.....	53
4.5 Soziale Auswirkungen.....	54
4.5.1 Computerkriminalität	54
4.5.2 Mobilität der Märkte.....	56
5 ELECTRONIC COMMERCE IN DER INFORMATIONSTECHNOLOGIE	57
5.1 Sicherheit und Vertrauen	57
5.1.1 Autorisierung	57
5.1.2 Verschlüsselung.....	58
5.1.3 Integrität	62
5.1.4 Authentisierung	63
5.1.5 Zertifikate	64
5.2 SmartCards	73
5.3 Elektronisches Bezahlen	79

5.3.1 Die einfachsten Varianten	81
5.3.2 Lastschriftverfahren	82
5.3.3 Kreditkartenbasierte Verfahren	83
5.3.3.1 FirstVirtual	83
5.3.3.2 CyberCash	85
5.3.3.3 SET	88
5.3.3.4 Zusammenfassung: Kreditkartenbasierte Methoden	92
5.3.4 Guthabekarten	92
5.3.4.1 Geldkarte	92
5.3.4.2 Andere kartenbasierte Zahlungsverfahren	96
5.3.5 Elektronisches Geld	97
5.3.6 Ecash-Feldtests der Banken	100
5.3.7 Andere Verfahren	102
5.3.7.1 Online-Inkassosysteme	102
5.3.8 Zusammenfassung	104
6 BUSINESS-TO-CONSUMER-COMMERCE	107
6.1 Die große Konvegenz	107
6.1.1 Zugangstechnologien zum Internet	108
6.1.1.1 Set-Top-Boxen	108
6.1.1.2 xDSL	109
6.1.1.3 Weitere Technologien	110
6.1.2 Next Generation Internet und Multimedia-Protokolle	110
6.1.3 Mobilfunknetze	112
6.1.4 Call-Center	113
6.1.5 Zukünftige Zugangstechnologien und Electronic Commerce	115
6.2 Online-Kataloge	116
6.2.1 Ein Beispiel	118
6.3 Profile und abgeleitete Daten	119
6.3.1 Warum Profile?	119
6.3.2 Cookie-Information	120
6.3.3 Web-Tracking, Kundenprofile & Marktanalyse	121
6.3.4 Web-Marketing und Banner-Werbung	122
6.3.5 Explizite Teilnehmerprofile	123
6.3.6 Abgeleitete Profile	123
6.3.7 Verdichtete Profilinformaton	124
6.3.8 Data Warehouses	124
6.4 Datenschutztechnologie für Kundenprofile	126
6.4.1 Die Perspektive des Verbrauchers: Datenschutz vs. Data Mining	126
6.4.2 OPS	127
6.4.2.1 Hintergrund	127
6.4.3 Organisatorische Betrachtung	128
6.4.4 P3P	129
6.4.4.1 Überblick	130
6.4.5 Bewertung: OPS und P3P im Vergleich	134
6.5 Virtuelle Shops & Malls	135
6.5.1 Shop-Architekturen und Varianten	139
6.5.2 Allgemeine Architektur für Online-Shops	140
6.5.3 Beispiel: Intershop 3	141
6.5.4 Oracle ICS	145
6.5.5 Shops für Jedermann	148
6.5.6 Was ist noch zu beachten?	148
6.6 Customer Relationship Management	150
7 BUSINESS-TO-BUSINESS-COMMERCE	152
7.1 Dokumentenaustausch beim Electronic Commerce	153
7.1.1 Elektronischer Datenaustausch	153
7.1.2 Open EDI	156
7.1.3 Interaktives EDI	157
7.1.4 Universal EDI	158
7.1.5 HTML als Alternative?	159
7.1.6 XML	162
7.1.7 XSL	165
7.1.8 XML/EDI	168
7.1.9 ICE – Information and Content Exchange	169
7.2 Extranets und Broker	174
7.2.1 Beispiele für Intranet- und Extranet-Anwendungen	177
7.2.1.1 Auktionen	177
7.2.1.2 Ausschreibungssysteme	177
7.2.2 Das Extranet auf neutralem Boden oder die neuen Mittler	179

7.2.2.1 Beschaffungssysteme	179
7.2.2.2 Broker.....	181
7.2.2.3 Der Trader.....	181
7.2.3 Zusammenfassung	183
7.3 Business Objects.....	183
7.3.1 Java Beans	185
7.3.2 Enterprise Java Beans	189
7.3.3 Die CORBA Business Object Component Architecture	191
7.3.4 Das San Francisco-Framework von IBM.....	200
7.3.5 Zusammenfassung	201
7.4 Workflow-Management zwischen Unternehmen	201
7.4.1 Allgemein	202
7.4.2 Beispiele	202
7.4.3 Open EDI?	202
7.4.4 Open Trading Protocol?	202
7.5 Elektronische Verträge.....	202
7.5.1 Vertragsformen	203
7.5.2 Tansaktionsphasen.....	205
7.5.3 COSOMOS – Ein Internet-Dienst für das Electronic Contracting	206
7.5.4 Ein Objektmodell für elektronische Verträge	207
7.5.5 Die COSMOS-Architektur.....	208
7.5.6 Weitere Entwicklungen im Bereich elektronischer Verträge	210
7.6 Zusammenfassung	211
8 ANWENDUNGEN IM B2B-COMMERCE	152
8.1 Supply-Chain-Management	214
8.2 Handel.....	214
8.3 Banken und der Wertpapier-Handel	215
8.4 Amazon.Com.....	217
8.5 Weiteres.....	217
8.5.1 Die Zukunft des Business-to-Business-Commerce	217
9 WOHN FÜHRT ELECTRONIC COMMERCE?	218
9.1.1 Die Zukunft der Bank im Internet	218
9.1.2 Handel.....	219
9.1.3 Freier Handel mit Kundendaten?	220
9.1.4 Trusted Third Parties.....	221
9.1.5 Prozessintegration, Interorganisationales Workflowmanagement	222
9.1.6 Supply-Chain-Management	222
9.1.7 Web-Billing	224
9.1.8 Beispiele für Virtuelle Unternehmen	224
9.1.9 Enterprise-on-demand	226
9.2 Beispiele	226
9.2.1 Amazon.com (oder ähnlich)	226
9.2.2 parts.com (oder ähnlich)	226
9.2.3 MyWorld (oder ähnlich)	226
9.2.4 Virtueller Lebensmitteleinkauf	226
9.2.5 Online-Kauf von Briefmarken	227
9.2.6 Music-on-Demand	228
9.2.7 Elektronische Notare	228
9.3 Wohin führt Electronic Commerce	229
10 AUSBLICK.....	230
11 INDEX	231
12 LITERATUR.....	233
13 URLS	238
13.1 Electronic Commerce Allgemein.....	238
13.2 Sicherheit und Vertrauen	238
13.3 Zahlungsverfahren	239
13.4 Online-Shopping.....	241
13.5 Sonstiges.....	242

Abbildungsverzeichnis

<i>Abb. 1: Geschäftsbeziehungen und beteiligte Rollen</i>	9
<i>Abb. 2: Phasen einer Handelstransaktion</i>	13
<i>Abb. 3: Verteilung des B2C-Umsatzes 1997 und 2002</i>	22
<i>Abb. 4: Verteilung des Marktvolumen im Media/IT-Bereich 1997</i>	23
<i>Abb. 5: Zelluläres Modell der Unternehmenskooperation</i>	35
<i>Abb. 6: Beispiel für ein virtuelles Unternehmen</i>	37
<i>Abb. 7: Zertifizierungshierarchie</i>	69
<i>Abb. 8: Eine Sperrliste für X.509 Zertifikate</i>	70
<i>Abb. 9: Grundschema einer SmartCard</i>	73
<i>Abb. 10: Aufbau einer Java-SmartCard von GemPlus</i>	76
<i>Abb. 11: Nachrichtenfluß bei SET</i>	89
<i>Abb. 12: Das Dual Signature-Verfahren von SET</i>	89
<i>Abb. 13: Austausch von Zertifikaten beim SET-Protokoll</i>	90
<i>Abb. 14: Abläufe und Instanzen bei GeldKarten-Transaktionen</i>	93
<i>Abb. 15: Blind geleistete Unterschrift der Bank</i>	98
<i>Abb. 16: Zahlungsprotokoll bei Ecash</i>	98
<i>Abb. 17: Kosten bei Zahlungstransaktionen über unterschiedliche „Schnittstellen“ einer Bank</i>	105
<i>Abb. 18: Komponenten eines Call-Centers</i>	115
<i>Abb. 19: Anbieter- und Nachfragerkataloge auf dem elektronischen Markt</i>	117
<i>Abb. 20: Die Rolle des neutralen elektronischen Produktkatalogs</i>	118
<i>Abb. 21: Qualität und Anonymität von Benutzerprofilen</i>	120
<i>Abb. 22: Verhandlungsprotokoll von P3P</i>	133
<i>Abb. 23: Referenzarchitektur für Online-Shops</i>	141
<i>Abb. 24: Intershop-Architektur</i>	143
<i>Abb. 25: Nutzungsvariante der Intershop-Software „Inhouse-Hosting“</i>	144
<i>Abb. 26: Nutzungsvariante der Intershop-Software „Mall- und Abrechnungs-Provider“</i>	144
<i>Abb. 27: Nutzungsvariante der Intershop-Software „Nur Mall-Provider“</i>	145
<i>Abb. 28: Beispiele für die Erweiterung des Shop-Systems</i>	146
<i>Abb. 29: Katalogschema beim ICS</i>	146
<i>Abb. 30: Produkte, Product Items und Features beim Oracle ICS</i>	147
<i>Abb. 31: Integrationsaspekte beim B2B-Commerce</i>	152
<i>Abb. 32: Schema von EDI-Nachrichten</i>	155
<i>Abb. 33: Vollständiger Geschäftsprozeß und beteiligte EDI-Nachrichten</i>	156
<i>Abb. 34: Entwicklung von SGML, HTML und XML</i>	162
<i>Abb. 35: Internet, Intranet und Extranet</i>	176
<i>Abb. 36: Die Architektur von Java</i>	185
<i>Abb. 37: Bestandteile des Java-Bean-Framework</i>	187
<i>Abb. 38: Integration von Enterprise Java Beans in die Ausführungsumgebung des Containers</i>	189
<i>Abb. 39: Organisatorisches Modell bei Enterprise Java Beans</i>	191
<i>Abb. 40: Sitzungs- und Entity-Beans</i>	191
<i>Abb. 41: Die Object Management Architecture</i>	193
<i>Abb. 42: Erweiterungen von CORBA für Business Objects</i>	194
<i>Abb. 43: Bausteine der BOCA</i>	194
<i>Abb. 44: Adapter zwischen Kunden und Lieferanten</i>	196
<i>Abb. 45: Generieren von IDL-Code aus CDL-Code</i>	198
<i>Abb. 46: Der Spezifikationsprozeß vom UML bis zum lauffähigen Code</i>	198
<i>Abb. 47: Klassenhierarchie der San Francisco Foundation Classes</i>	200

<i>Abb. 48: Die Architektur des San-Francisco-Frameworks</i>	201
<i>Abb. XXX: Vertragsbeziehungen des Publikationsagenten</i>	204
<i>Abb. XXX: Vertragsbeziehungen zwischen Parteien</i>	206
<i>Abb. 49: Das COSMOS Vertragsmodell</i>	207
<i>Abb. 50: Funktionen des Electronic-Contracting-Systems</i>	210

1 Prolog im Jahre 2025

Bob ist Avatar-Designer und hat sein Gewerbe auf Mauritius angemeldet. Er ist Mitglied der „Gilde der Avatar-Designer™“. Als zünftiger e-Lance befindet er sich gerade auf dem Flug nach London, um seine Freundin zu besuchen. Sein Hauptgeschäft besteht im Abarbeiten von Aufträgen zur Spieleentwicklung, die sporadisch von wechselnden Produktionsunternehmen eintreffen. Er steht in Kontakt mit einigen Kollegen, mit denen er sich „per Knopfdruck“ zu einem virtuellen Designer-Verbund zusammenschließen kann. Einige sind auf die 3D-Modellierung spezialisiert, andere auf die Bitmaps, die als „Skin“ auf die Oberfläche des Avatars projiziert werden. Jeder Experte ist bei einem Broker mit seinen besonderen Fähigkeiten eingetragen. Dazu zählen auch seine Security-Präferenzen, die bevorzugte Währung sowie Zertifikate und Auszeichnungen. Bob rechnet in Cayman-Cash ab, bevorzugt verschlüsselte Kommunikation, hat sich aber ansonsten für die von der Cayman Virtual betriebene „Low-Cost Economy“ entschieden. Dies hilft, unnötige Kosten bei der Kooperation mit Geschäftspartnern zu sparen. Hin und wieder kommt es jedoch zu Problemen mit unseriösen Partnern, die Bob jedoch bereit ist, in Kauf zu nehmen.

Seitdem das Unternehmen *Microlaw* Branchenkomponenten für Soft-Good-Designer vermarktet, besteht jederzeit die Möglichkeit, vollständige Aufträge ad hoc über diese Software abzuwickeln. Ein Designer, der Vakanzen für einen nachgefragten Zeitraum besitzt, kann sogar die Entscheidung, einen Vertragsvorschlag zu akzeptieren, an seinen elektronischen Verhandlungsagenten delegieren. Bob akzeptiert beispielsweise nur Aufträge ab 300 Euro pro Tag. Wenn allerdings ein Auftrag für mehr als 15 Tage angeboten wird, ist er verhandlungsbereit und läßt sich von seinem Agenten in den Vertragsprozeß einbeziehen. So auch beim aktuellen Auftrag:

Anhand der Auftragspezifikation ist zu erkennen, daß 25 Avatare innerhalb von 10 Tagen zu entwickeln sind. Dazu muß Bob einige Kollegen einbeziehen, da er allein pro Avatar einen ganzen Tag benötigen würde. Bob erkennt darüber hinaus, daß eine gemischte Expertise aus 3D- und Oberflächendesign erforderlich ist. Kürzlich war für ein anderes Projekt eine ähnliche Kombination erforderlich. Bob wählt den alten Vertrag aus und ersetzt seine Leistungspezifikation mit den Konditionen der Softwarefirma. Diese schreiben eine Fertigstellung des Auftrags innerhalb von 10 Tagen vor. Er ändert diesen Teil der Spezifikation ab in 8 Tage, um Luft für Nachzügler und Qualitätskontrolle zu gewinnen. Außerdem reduziert er den Tagessatz auf 250 Euro. Pro Avatar kalkuliert er jeweils einen Personentag für das 3D-Modell sowie einen für die Oberfläche. Diese Daten trägt er in die Spezifikation für Unterauftragnehmer ein.

Mit Hilfe eines Brokers werden 105 Anbieter ermittelt, die jeweils Kapazität für bis zu drei Avatare besitzen. Mit Hilfe einer Ranking-Software, die Bob für einen Euro pro Benutzung mietet, stuft er die Angebote nach Tagessatz, zertifizierter Qualität und persönlicher Bekanntheit ein. Dabei lassen sich mit den 14 besten Designern bereits 21 Avatare abdecken. Da er das Risiko für kalkulierbar hält, läßt er die restlichen drei per Auktion ausschreiben. Er konfiguriert das Bewertungssystem nach Qualität (70%) und Tagessatz (30%). Als Ergebnis wird ein international bekannter Avatar-Designer mit einem Tagessatz von 500 Euro anhand einer umgekehrten holländischen Auktion vermittelt. Er koppelt den Untervertrag mit diesem Designer an sein eigenes Angebot an die Softwarefirma und gibt „seinen“ Vertrag zur Notarisierung frei. Wenige Sekunden später wird dieser Abschluß an das Produktionsunternehmen gemeldet, dessen Vertrag damit ebenfalls geschlossen wird. Bob hat damit Glück gehabt, da gleichzeitig noch vier weitere Konsortien an der Formierung einer virtuellen Organisation für diesen Auftrag gearbeitet hatten.

Aus dem abgeschlossenen, führenen Vertrag übernimmt er die bereits existierende Workflow-Definition, die ein zweistufiges Vorgehen vorsieht, zur Abwicklung des Auftrags: in der ersten Phase werden am ersten Tag die (vom Kunden erhaltenen) schriftlichen Spezifikationen der Charaktere an alle Auftragnehmer herausgegeben. Zwei Tage später erwartet Bob die Resultate zurück. Dabei stellt die Vertragsspezifikation sicher, daß 3D- und Oberflächendesigner, die jeweils am gleichen Modell arbeiten, über einen gemeinsamen Workspace Daten austauschen können. Wenn ein Resultat von einem Auftragnehmer zurückgeliefert wird, kommentiert Bob das Ergebnis. Die Workflow-Software kümmert sich um die Weiterleitung des Kommentars an den Designer. Dies erfolgt jedoch erst, wenn alle Entwürfe eingetroffen sind und kommentiert wurden. Jeder Autor erhält am fünften Tag alle Entwürfe und kann diese sowie Bobs Kommentar für die Überarbeitung seines eigenen Entwurfs berücksichtigen. Am 8. Tag liegen die endgültigen Resultate bei Bob vor, der abschließend noch einzelne Korrekturen vornimmt. Am neunten Tag liefert er das Ergebnis an die Softwarefirma.

Laut Vertragsentwurf war ein Zahlungsziel von 5 Tagen nach Lieferung vorgesehen. Entsprechend erhält Bob die Zahlung fristgemäß am 14. Tag. Aufgrund der vertraglich fixierten Tagessatzvereinbarungen kann Bobs Software die korrespondierenden Teilzahlungen unmittelbar an die Auftragnehmer weiterleiten. Eine Konvertierung von Cayman-Cash in die jeweiligen bevorzugten Währungen erfolgt automatisch zum fixierten Kurs am Tag des Vertragsschlusses. Am selben Tag noch wird die Transaktion damit vollständig abgeschlossen.

Vorwort

In der kurzen Geschichte der Informatik trafen wir immer wieder auf Modewörter und Versprechen, von denen wir technische Innovationen, substantielle Erkenntnisprünge oder eine sonstige Verbesserung unseres täglichen Lebens erwartet hatten. Management-Informationssysteme, Expertensysteme, Meta-Meta-Modellierung – all dies sind Beispiele dafür. In der Regel hatten diese Entwicklungen nur marginale Auswirkungen auf das tägliche Leben – und wenn, hat ihre Durchdringung sehr viel länger gedauert, als von den geistigen Vätern erwartet. Erst heute kann man beispielsweise von Data Warehouse-Anwendungen hilfreiche Informationen zur Unternehmensanalyse und -steuerung erwarten. In der 30jährigen Geschichte der Management-Informationssysteme, Unternehmenslagezentren, Executive Information Systems etc. scheiterte die Umsetzung immer wieder an mangelnder Standardisierung, zu hoher Hardware- und Softwarekosten bei zu geringer Leistungsfähigkeit.

Wird auch Electronic Commerce eine 30jährige Entwicklung benötigen? Sind die Wachstumsprognosen von Forrester, Ovum & Co so maßlos übertrieben, daß erst in 30 Jahren das versprochene Marktvolumen erreicht wird? Wird Electronic Commerce deswegen an uns vorüberziehen, ohne daß wir es im täglichen Leben spüren? Sicherlich nicht, denn einerseits gibt es Electronic Commerce bereits seit vielen Jahren, andererseits setzen sich neue Electronic Commerce-Technologien und -Geschäftsmodelle so schnell durch, daß Analysten sie gar nicht mehrere Jahre im voraus exakt prognostizieren können.

Der virtuelle Raum des elektronischen Handels entstand bereits zaghaft und hoffnungsvoll in den 70er Jahren durch die Einführung von EDI-Systemen. Die Vision war, alle Handelsunternehmen miteinander über standardisierte Dokumentenformate interoperabel zu machen. Daraus wurde bisher lediglich ein Alptraum: Wie auf einer römischen Galeere rudern Hundertschaften von Consultants, Entwickler, Analytiker usw. gleichzeitig an der Realisierung einzelner, gigantischer EDI-Transaktionssysteme, nur um für ein individuelles Großunternehmen eine individuelle Lösung zu schaffen, die allerdings nicht kompatibel ist mit der individuellen Lösung eines anderen. Ein ähnlicher Aufwand kann nochmals für die Gesamtheit aller EDI-Systeme der meist kleineren Geschäftspartner erwartet werden. Daß Electronic Commerce jedoch naturgemäß unternehmensübergreifend stattfindet und daher technische und inhaltliche Interoperabilität zwischen Kooperationspartnern erfordert, wird vom individuellen Unternehmen im Eifer des Wettbewerbs schnell vernachlässigt: der kurzfristige Vorteil der schnellen Lösung setzt sich somit in der Praxis immer gegenüber dem größeren, langfristigen durch. Die Ursache liegt – zumindest im EDI-Bereich – nicht zuletzt an der Fehlinterpretation der Marktkräfte sowie bei Designfehlern des Standardisierungsprozesses selbst.

Der EDI-Marktplatz entwickelte sich folglich zunehmend zu einem Boxkampf, dessen Spielregeln eher von den Schwergewichten als vom Ringrichter bestimmt werden. Erst seit der breiten Nutzung des Internet entzerrte sich dieses Bild und Electronic Commerce wurde tatsächlich zu einem „Massenmarkt“ mit Chance auf Effizienz, Evolution und Fairness.

Im Kontext des Internet ist Electronic Commerce im Gegensatz zum EDI ein Phänomen, das erst aus dem Zusammenspiel unterschiedlicher Technologien entstehen konnte: Ohne das Zusammentreffen von Internet, World Wide Web, preiswerter Hardware und Software sowie dem Wettbewerbsdruck auf Unternehmen, ihre Geschäftsprozesse mit anderen zu integrieren, hätte es nicht zu der breiten heutigen Ausfächerung von Electronic-Commerce-Schwerpunkten kommen können. Nur durch diese Rahmenbedingungen konnten sich auch Kleinunternehmen gegenüber den Großen emanzipieren, da sie im Kontext der Internet-Ökonomie als flexiblere Einheiten Innovationen meist schneller durchsetzen können.

Vor diesem Hintergrund einer Internet-Ökonomie befassen wir uns mit elektronischen Zahlungsverfahren wie eCash, CyberCash, SET. Vor allem melden aber auch die Notenbanken ein vitales Interesse an diesem Thema an. SmartCards, Online-Shops, Data Mining von Profilinginformationen, 1:1 Marketing, Datenschutzfragen, TrustCenter beschäftigen Online-Anbieter heute im Internet im Rahmen des *Business-to-Consumer-Commerce* und Themen wie Brokerage, Electronic Contracting, Online-Auktionen, Beschaffungssysteme, Vertrauensinfrastrukturen, Enterprise Java Beans etc. sind relevant für den sog. *Business-to-Business*-Bereich. Java, XML und CORBA dienen dabei als moderne technische Middleware.

Electronic Commerce findet damit in einem technischen und gesellschaftlichen Kontext der *Konvergenz* statt: Grenzen zwischen ehemals isolierten Fachgebieten verwischen. Rollen sind nicht mehr konstant zuzuordnen, Medien verschwimmen zu einem amorphen Multimedialium. Wettbewerber sind nur noch Mausklicks voneinander entfernt. Diesen Prozeß beschreiben die Autoren Davis und Meyer sehr treffend in ihrem Buch „Blur“ – was soviel heißt wie *verwischen*: In der Blur-Wirtschaft

- verwischen die Grenzen zwischen Käufer und Verkäufer: es tritt der Lebensmittelkonzern als Kunde seines Händlers auf, um Regalfläche anzumieten,
- wird über das Internet ferngesehen und mit dem Fernseher Zeitung gelesen,
- verwischen die Grenzen zwischen Organisationen und Personen: Individuen schließen sich ad hoc zu *virtuellen Unternehmen* zusammen und die Persönlichkeit des Individuums tritt zunehmend aus der Organisation hervor,
- werden Handelsmechanismen des Finanzmarktes für den Einkauf von Dienstleistungen eingesetzt, und Finanzdienstleistungen sind wie ein Automobil konfigurierbar,
- verwischen Ausbildung und berufliche Praxis – wir lernen, lehren und beraten fast jeden Tag gleichzeitig,
- verwischen schließlich geographische, nationalstaatliche und organisatorische Grenzen.

Über ECommerce-Anwendungen und mögliche Effekte dieser Verwischungen lesen wir täglich in der Presse. Dazu einige Beispiele:

- Pharmakonzerne nutzen *Data-Mining*-Software, mit denen der Verlauf eines Grippe-Virus als Wolke anhand von Arzneiverkäufen visualisiert werden kann. Der Grippevirus kann damit wie ein Wetterbericht für einzelne Orte vorhergesagt werden. Dabei lassen sich wertvolle Informationen darüber gewinnen, wie am folgenden Tag Auslieferungslager und Apotheken optimal zu beschicken sind – Information gewinnt somit immer mehr Bedeutung als vierter, elementarer Wirtschaftsfaktor.
- Debis und Metro richten mit 90 Mio. DM Budget einen *virtuellen Supermarkt* mit Couriersdienst ein. Lieferdienste, Supermärkte, Lagerlogistik, Internet, Zahlungs- und Inkassofunktionen verschmelzen dabei.
- *Auktionssysteme* werden überall dort eingesetzt, wo Güter mit einfacher Produktspezifikation gehandelt werden: Büromaterial, Mineralöl oder Flugtickets. Als Handelspartner treten hierbei Konsumenten und Konzerne gleichermaßen auf.
- Ein *Notar* wird sich als Folge des Signaturgesetzes in Zukunft möglicherweise mit allen möglichen Anwendungen rechtskräftiger elektronischer Unterschriften beschäftigen müssen. So besteht die Möglichkeit, daß auch elektronisch verfaßte und signierte Verträge auf elektronischem Wege beurkundet werden können.
- In *aktuellen Feldtests der Banken* werden mit mehr oder weniger Erfolg elektronische Zahlungsmittel eingeführt. Dabei kann die Verschmelzung aus Internet, Fernsehen und Spielekonsolen innerhalb weniger Monate zu völlig neuen Situationen führen. Man stelle sich vor, Nintendo oder Sony führen innerhalb kurzer Zeit für 15-20 Mio. Spielekonsolen einen geschlossenen, virtuellen Marktplatz im Internet mit eigenem Währungsraum ein...
- Oder was passiert eigentlich, wenn sich eine Offshore-Bank entschließt, *privates elektronisches Bargeld* international in Umlauf zu bringen? Dann konkurriert plötzlich privatwirtschaftliches mit nationalem Notenbankgeld. Ist dies ein Horrorszenario? Oder können Privatwährungen als Regulativ dienen, das andere Volkswirtschaften über die Wechselkurse und durch „Abstimmung mit den Füßen“ im Zaum hält?
- IBM entwickelt mit dem *San Francisco Framework* ein Java-basiertes Konkurrenzprodukt zu SAP, das eine Ad-hoc-Integration sog. Business Objects zwischen Unternehmen erlaubt. In Verbindung mit einer Standardisierung dieser Objekte besteht damit erstmalig die Möglichkeit, im Bereich des Business-to-Business-Commerce Softwaresysteme zur Laufzeit direkt zu verbinden.
- Der Bereich des *Datenschutzes* wurde lange Zeit vernachlässigt. Hier konnten Anbieter von Shops und Onlinediensten – zumindest in den USA – Kundendaten beliebig verarbeiten und kommerziell verwerten. Heute werden jedoch Protokolle entwickelt, mit denen persönliche Daten nur kontrolliert und gegen Vorlage einer zertifizierten Datenschutz-Policy an Online-Betreiber herausgegeben werden können. Adresseninformation wird damit erstmals auch für den Kunden ein handelbares Gut.

Diese Beispiele bieten nur einen schillernden Überblick. Dabei lassen sich bereits unterschiedliche Perspektiven und gesellschaftliche Rollen im Zusammenhang mit dem Electronic Commerce unterscheiden:

- *Juristen* sind gefragt, Phänomene des EC so in einem justiziablen Rahmen zu fassen, daß für Konsumenten, Anbieter und Mittler Rechtsverbindlichkeit und Rechtssicherheit gewährleistet werden kann.
- *Politiker* sind gefragt, einen regulatorischen Rahmen zu schaffen, der die freie und faire Entfaltung des Elektronischen Marktes weder behindert, noch ihn zum Wilden Westen ausarten läßt.
- *Volkswirte* interessiert z.B. die Auswirkung elektronischen Geldes sowie die zunehmende Mobilität der Wirtschaftsfaktoren Arbeit, Kapital und Information.

- Das *Unternehmensmanagement* ist dank moderner Netzwerk- und Softwaretechnologie mit verfeinertem Rüstzeug zur betrieblichen Organisation ausgestattet. Damit lassen sich sehr viel exaktere Marktanalysen, neue Geschäftsmodelle oder erfolgreichere Kooperationsformen verwirklichen.
- Schließlich obliegt die *Realisierung* von Electronic-Commerce-Systemen denen, die sich mit technischen Fragen der Kommunikation, der Informationsverarbeitung sowie der Kollaboration zwischen Menschen und Maschinen beschäftigen – und das sind *Informatiker*.

Electronic Commerce – für wen?

Es ist heute noch nicht generell abzusehen, wer eigentlich Nutznießer des Electronic Commerce ist: Sind es Kunden und Konsumenten, die günstigere Einkaufskonditionen vorfinden? Sind es Banken und Handelsmittler, die an einem erhöhten Aufkommen von Internet-Handelstransaktionen mitverdienen? Sind es vielleicht nur einige Internet-Startup-Unternehmen, die sich über ihre Produkte die Effizienzsteigerung des Marktes auszahlen lassen? Sind es die USA, wo fast ausschließlich international genutzte Software produziert wird, oder vielleicht Schwellenländer, die nun zu Billigkonditionen Produkte und Dienstleistungen anbieten und abrechnen können? Genaues kann heute niemand sagen. Jedenfalls steht für vielerlei Spekulationen noch der Beweis ihrer Wirtschaftlichkeit aus: Beispielsweise werden wohl manche Verfahren für ‘Micropayment’-Systeme Forschungslabors und Feldtest nicht verlassen können, wenn eine Bezahlung im Werte von fünf Pfennigen 30 Pfennig Transaktionskosten mit sich bringt. Dies liegt weniger am Preis der Technik als an dem der Sicherheit sowie an dem Geschäftsmodell.

Nur eines ist heute klar erkennbar: Nachdem technologisch der Weg zum elektronischen Handel grundsätzlich geebnet werden kann, wird die Frage nach der Vertrauensinfrastruktur immer brennender. Der Verlust einer elektronischen Münze kann toleriert werden, wenn der Händler oder die Bank die Kosten trägt. Demgemäß wird ein unbekannter Shop-Betreiber größere Chancen auf Kundschaft haben, wenn er z.B. bei einer Bank als Vertrauensspender unterschlüpft und diese das Transaktionsrisiko trägt (Kartendiebstahl, Untergang des Anbieters oder Betrug durch den Anbieter). Natürlich wird sich die Bank dieses Vertrauen vom Shop-Betreiber vergüten lassen – Vertrauen ist damit ein handelbares Gut geworden. Damit dürfte auch der kommerzielle Umgang mit Vertrauen noch längerfristig ein aktuelles Thema für Forschung, Entwicklung und zukünftige Geschäftsmodelle sein.

Daraus ist zu vor allem folgern, daß Electronic-Commerce-Software nur unter Berücksichtigung ökonomischer, juristischer und sozialer Randbedingungen realisiert werden kann. Eine technikverliebte Perfektionierung von Sicherheitsmechanismen nützt nichts, wenn diese Sicherheit nicht auch vom Benutzer wahrgenommen wird. Dies bedeutet wiederum, daß eine Behandlung des Thema „Electronic Commerce“ unbedingt ganzheitlich erfolgen sollte, um diese Randbedingungen bewußt zu machen.

Gleichzeitig kann ein technisch detaillierter Überblick über Entwicklungen im Electronic Commerce jedoch nur als Momentaufnahme verstanden werden. Da dieses Gebiet im Spannungsfeld aus Politik, Ökonomie und Informationstechnologie mit unterschiedlichsten Anforderungen und Potentialen konfrontiert ist, wird sich an diesem Zustand auch in den nächsten Jahren nicht allzuviel ändern. Vielmehr werden durch die Vermischungen unterschiedlicher Technologien (z.B. Internet und TV), Rollen (z.B. Käufer/Verkäufer) und Organisationsformen (Unternehmen/Einzelperson) spontan immer wieder neue Geschäftsmodelle und Nutzungsformen entstehen.

Ein Buch kann also ebenfalls immer nur eine solche Momentaufnahme sein. Ein Buch im herkömmlichen Sinne ist somit ein eher archaisches Instrument für den Transport von Information und Wissen. Folglich versuche ich mit diesem Buch einige „Added-Values“ zu verbinden, die auch eine langfristige Attraktivität sichern sollen:

- Es soll Spaß machen, dieses Buch zu benutzen. Daher habe ich einen weniger scientistischen Stil gewählt als den, der üblicherweise in Forschungsberichten, Dissertationen und Diplomarbeiten anzutreffen ist. Schließlich sollte es auch Spaß machen, dieses Buch zu schreiben – und das ist vor allem dann der Fall, wenn es möglichst viele erreicht, für möglichst viele relevant ist und schließlich auch von möglichst vielen verstanden wird.
- Diese Buch lebt weiter, indem ich die hier begonnene Sammlung von Artikeln und Referenzen im Internet fortsetze. Unter der Adresse <http://www.XXXXXXX.de> wird in Kürze ein EC-Online-Forum entstehen, das der Leserschaft und jedem Interessierten als Plattform zur Weiterbildung dient.

Aufbau des Buches

Mit diesem Buch möchte ich einen Überblick über die mir bekannten technologischen und organisatorischen Aspekte des EC geben. Dabei ist es sinnvoll, das Thema zunächst durch eine Klassifikation dieser Aspekte be-

grifflich besser zu fassen. Anschließend wird im Kapitel XXX ein Überblick über den ökonomischen Hintergrund des EC vermittelt, damit für die nachfolgenden technischen Betrachtungen im Kapitel XXX eine klarere Zielsetzung und ein schärferer Bewertungsrahmen gegeben werden kann. Nachdem somit „von oben“ im Sinne *volkswirtschaftlicher* und „von unten“ im Sinne *technologischer* Rahmenbedingungen das Spannungsfeld aufgebaut wurde, steht schließlich im Kapitel XXX das *Unternehmen* im Vordergrund und seine Möglichkeiten, auf dem elektronischen Marktplatz zu agieren.

XXX

Ein Buch wie dieses besitzt ein „Fenster“ von vielleicht 2-3 Jahren – danach werden neue Technologien, neue „Business Models“ und sogar Gesetzgebungen seine Aktualität immer mehr angreifen. Sie mögen sich also fragen, ob ein Buch (an dem man ja auch eine gewisse Zeit schreibt) überhaupt noch eine adäquate Publikationsform darstellt angesichts einer überbordenden Fülle von Informationen im WWW. Im Prinzip haben Sie recht. Ich habe mich bei der z.T. beschwerlichen Zeit des Schreibens einige Male gefragt, ob es nicht sinnvoller wäre, den Inhalt in Form kleiner Fragmente (sprich: HTML-Seiten) über das Netz verfügbar zu machen. Wenn dann die RSA-Schlüssellänge, die als sicher angenommen wird, von 768 auf 1024 Bit steigt, ist nur eine kurze Aktualisierung erforderlich. Allerdings konnte ich mir die gegenteilige Antwort selbst während des Schreibens geben: Durch die immense Interdisziplinarität dieses Themas kommt es immer wieder zu unerwarteten Berührungspunkten ganz unterschiedlicher Themen, sobald man sich von seiner fachlichen „Home Base“ durch den Morast aus Recherche und täglicher Praxis zu den entlegendsten Gebieten des Electronic Commerce vorantastet. Die Kombination von Disziplinen führt dabei zu einer schier unerschöpflichen Fülle von Themen im Bereich der Forschung und Praxis. Hier nur einige Beispiele:

- Datenschutzforderungen + XML + WWW → Neue Geschäftsmodelle bei Nutzungsprofilen
- Internationalisierung + WWW + Signaturgesetz → Neue Geschäftsmodelle des Electronic Contracting
- Kostenreduktion im IT-Bereich + Internet + 12 Millionen Internet-Nutzer in Deutschland → Lufthansa's InfoFlyway

Der Mehrwert eines Buches liegt also in der Schaffung einer monolithischen Wissensgebäudes, das zwischen seinen fragmentierten Fakten ein enges Beziehungsgeflecht webt. Ein Buch kann somit fernab des täglichen Internet-Rauschens gelesen und hoffentlich auch verdaut werden.

Dieses Buch kann aufgrund seines Umfangs nicht alle Technologien, Anwendungen und Auswirkungen in jeder detaillierungsstufe adressieren. Es wird jedoch der Versuch unternommen, die Brücke zu schlagen zwischen Grundlagen im technologischen und im ökonomischen Bereich. Dabei werden traditionelle Ansätze den neuen der Internet-Ökonomie gegenübergestellt. Das Buch dient damit nicht nur als Nachschlagewerk im Sinne eines erweiterten Glossars, sondern insbesondere als Lektüre, die den Leser durch mitunter recht nebulöse und leider stark überhitzte Themenkomplexe führen soll. Als Resultat ist dabei zu hoffen, daß nicht nur der Wunsch nach gezieltem Nachschlagen befriedigt werden kann, sondern auch die allgemeine Leselust.

Da sich aber die Problematik des Zeitfensters nicht wegdiskutieren läßt und zudem jemand, der sich dem Thema Electronic Commerce widmet, dies auch mit Taten belegen sollte, habe ich mir ein Business Modell einfallen lassen, dessen Prüfung erst erfolgen kann, wenn schon lange kein Einfluß auf den Inhalt genommen werden kann: über die Web-Site www.XXX.de wird der Inhalt von mir weitergepflegt und steht allen Käufern des Buches kostenlos zur Verfügung. Daß ich mir dennoch bei diesem Geschäftsmodell einen Gewinn verspreche, werde ich nach getaner Arbeit im Ausblick ganz am Ende erklären.

Bevor es richtig losgeht...

... noch einige Worte zum Buch und seiner Entstehung:

Dies ist keine Dissertation! Ich habe aus ökonomischen Gründen bewußt die Meßlatte auf 95% und nicht auf 100% gesetzt, sonst hätte das Buch weit nach seinem Zeitfenster erschienen müssen. Diese Maßnahme hilft mir, die Zeit im wesentlichen auf den Inhalt und erst in zweiter Linie auf vollständige Unterfütterung mit Literaturreferenzen und sonstigen Belegungen vielleicht etwas kühner Thesen zu verwenden. Dafür steigert es auch den Schreibspaß, hier und da Zynismen und ironische Bemerkungen einzubauen – die wissenschaftliche Community möge es mir verzeihen!

An einem Buch sind beliebig viele Personen beteiligt, so auch hier: folglich möchte ich allen danken, die mitgeholfen haben an seiner Korrektur und Fertigstellung. Dies gilt vor allem Christa Preisendanz vom dpunkt-Verlag und ihren Mitarbeitern sowie XXX.

Dieses Buch wäre aber gar nicht erst zustande gekommen, wenn ich mich nicht bereits vor einigen Jahren für die

Weiterarbeit an der Uni Hamburg entschieden hätte. Die dortige Arbeitsgruppe VSYS (Verteilte Systeme) unter der Leitung von Prof. Lamersdorf bot die Möglichkeit zur der freien Entfaltung neuer Ideen sowie die Zusammenarbeit mit Fachkollegen. Dieses Buch ist bereits Nummer drei aus einer Serie von dpunkt-Publikationen innerhalb eines Jahres [Grif98, Boge99] – und ein Ende ist noch nicht in Sicht [Grif99??? XXX].

Ein wichtiger Einfluß war und ist die Arbeit bei Ponton Hamburg, einem Software-Unternehmen mit einer seltenen Kombination aus Kreativität, Effizienz und Kompetenz. Durch den engen Kontakt zu Ponton seit dem Jahr 1996 entstand eine Synergie aus Theorie und Praxis, die zur gegenseitigen Befruchtung führte. Meine „Denke“ und „Fühle“ wurde dabei insbesondere inspiriert von Salvatore Vanasco, einem selten gewordenen Tausendsassa, dem ich als unerschöpfliche Quelle der Inspiration zu Dank verpflichtet bin.

Nur in einem solchen Biotop konnte schließlich das COSMOS-Projekt entstehen: Zum einen eher grundlegend orientierte Forschung an der Uni, jedoch mit konsequentem Fokus auf das ökonomisch Sinnvolle, zum anderen vorwettbewerbliche Entwicklung bei Ponton, kombiniert mit der Vision einer gesellschaftlichen Formung durch die Idee des „Electronic Contracting“. Die dritte Komponente ist dabei Europa – konkret die Europäische Kommission, mit der ich im Rahmen dieses Projekts zusammenarbeite. Auch hier sind es wiederum Personen mit Visionen und gestalterischem Impetus, die leider zu häufig durch das Bild in der Öffentlichkeit verzerrt werden, wenn die großen Nachrichten die Ergebnisse mühseliger Kleinarbeit überlagern.

2 Was ist Electronic Commerce?

Wenn wir ein Buch online bestellen, wenn ein mobiler Agent zum Suchen und Bezahlen von CDs ausgesendet wird, wenn die Lufthansa Flugtickets über das Internet versteigert, wenn Apotheken nicht mehr beim Großhändler, sondern direkt beim Hersteller ihre Arzneimittel bestellen, wenn Softwarekomponenten verschiedener Unternehmen sich über Produktspezifikationen verständigen, wenn eine komplexe Dienstleistung von einem virtuellen Unternehmen aus 15 Kleinunternehmen in Ad-hoc-Kooperation erbracht wird, wenn elektronische Notare Online-Verträge beglaubigen, wenn sich die Bundesbank Gedanken macht über die Geldmenge und Mittel ihrer Steuerbarkeit, wenn die Clinton-Administration eine Internet-Besteuerung aufhebt, so hat dies alles mit Electronic Commerce zu tun.

Es ist damit unschwer zu erkennen, daß dieses Thema nicht nur aufgrund seiner Interdisziplinarität besonders komplex ist, sondern auch wegen der rasanten Entwicklung des Internet und seiner EC-Anwendungen. Die direkten oder indirekten Auswirkungen des EC werden heute bereits heiß diskutiert: Billionen-Umsätze im Jahre XXXX (Forrester-Studie), Arbeitslosen-Quoten in zweistelliger Höhe ("Globalisierungs-Falle"), Rationalisierungseffekte durch Standardisierung und Globalisierung etc.

2.1 Einführung

...

Definitionen

Der Begriff des "Electronic Commerce" kann über seine allgemeine *Intention* oder auch anhand seiner Anwendungsfelder definiert werden: Im ersten Fall würde die Definition etwa

"Die Unterstützung von Handelsaktivitäten über Kommunikationsnetze"

lauten. Unterschiedliche Anwendungsbereiche wie "Elektronische Zahlungsverfahren", "Shopping Malls", "Electronic Data Interchange" könnte man daraus ableiten. Die intensionale Definition ist allerdings sehr abstrakt und damit kaum greifbar. Eine *extensionale* Definition würde entsprechend versuchen, Electronic Commerce über die Summe seiner Technologien und Verfahren zu definieren. Hier besteht damit das Problem, nicht alle Aspekte erfassen zu können. Versuchen wir es dennoch mit einer solchen Definition, erhalten wir fast schon ein Inhaltsverzeichnis für dieses Buch. Daher hat eine derartige Definition für den Autor gewissen Wert ;-)

"Electronic Commerce ist der Einsatz von Internet-Technologien, Sicherheitsinfrastrukturen, digitalem Geld, Electronic Shopping Malls, Electronic Data Interchange, SmartCards, mobilen und/oder intelligenten Agenten, Verhandlungsprotokollen und -strategien, elektronischen Notaren, Zertifizierungsautoritäten, interorganisationales Workflow-Management, elektronischen Verträgen zur Anbahnung und Durchführung von Handelstransaktionen im Internet."

Da auch diese Definition unhandlich – weil schnell veraltet – ist, soll unsere Definition und damit die Klassifikation von EC-Technologien zunächst in mundgerechte Teile zerlegt werden. Dazu verwenden wir im wesentlichen folgende Klassifikationen:

1. *Akteure* einer Handelstransaktion
2. *Phasen* einer Handelstransaktion
3. *Volumen* einer Handelstransaktion
4. *Architekturelle Ebenen* von EC-Software

2.2 Klassifikationen

2.2.1 Akteure und Rollen beim Internet-Handel

Als EC-Akteure treten Marktteilnehmer auf, die im allgemeinen in zwei Rollen agieren:

- **Käufer**, auch Kunde oder Konsument genannt.
- **Verkäufer**, auch Händler (engl. *Merchant*) genannt.

Diese Rollen können von Geschäft zu Geschäft wechseln. Wir können dabei Akteure als juristische Personen auffassen, die sich wiederum in natürliche Personen (also Menschen) und Organisationen (Unternehmen, Vereine, staatliche Körperschaften etc.) unterteilen. Je nachdem, welcher dieser Ausprägungen die beiden Geschäftspartner angehören, kann es zu unterschiedlichen Ausprägungen einer solchen Zweierbeziehung führen:

- Consumer-to-Consumer-Commerce (C2C).
- Business-to-Consumer-Commerce (B2C).
- Administration-to-Consumer-Commerce (A2C).
- Administration-to-Administration-Commerce (A2A).
- Business-to-Business-Commerce (B2B).
- Business-to-Administration-Commerce (B2A).

Nur einige dieser Ausprägungen sind von praktischer Relevanz; daher werden im folgenden vor allem die Bereiche B2B, B2C und B2A erläutert. Der Bereich des *Business-to-Consumer-Commerce* zielt dabei auf den Online-Handel zwischen Händlern und Privatpersonen ab. Dabei sind solche Handelstransaktionen durch Spontaneität und eher mittlere bis kleine Transaktionsvolumina gekennzeichnet. Üblicherweise findet neben der Produktauswahl und möglicherweise der Auslieferung vor allem auch die Bezahlung online statt. Beim *Business-to-Business-Commerce* besteht in der Regel eine längerfristige Geschäftsbeziehung zwischen den Transaktionspartnern. Traditionell erfolgt dies zunächst entlang der Zulieferbeziehung einer bestehenden Wertschöpfungskette (siehe auch weiter unten zu *Supply Chain Management*). Dabei steht nicht nur die vollständige Abwicklung der Transaktion im Vordergrund als die Schaffung flexibler Kooperationstechniken zwischen den jeweils beteiligten IT-Systemen (siehe auch: *Extranet*). Als dritter dominanter Bereich sollte der des *Business-to-Administration-Commerce* erwähnt werden, bei dem im wesentlichen als Anwendungsbereich das öffentliche Beschaffungswesen im Vordergrund steht. Durch Anwendungen wie z.B. Auktionssysteme wird hierbei ein höheres Maß an Transparenz und damit auch an Transaktionseffizienz geschaffen. Zu beachten ist jedoch auch, daß eine beliebige Vermischung der genannten Rollen und Beziehungen die Regel bestätigen: Bei Unternehmen ist der Einsatz elektronischer Beschaffungssysteme zunehmend üblich, wie der Einkauf etwa von Literatur über Online-Shop, wie etwa Amazon.de. Umgekehrt besteht für Konsumenten die Möglichkeit, Produkte über Auktionssysteme zu erwerben (z.B. Lufthansa Info-Flyway) oder als Einzelunternehmung etablierte Geschäftsbeziehungen zu einem festen Stamm von Geschäftspartnern zu pflegen. Somit kann die Trennung zwischen B2C und B2B folgendermaßen vorgenommen werden: Während beim B2C-Commerce der Online-Kauf durch den menschlichen Benutzer als vorherrschendes Muster dient, steht beim B2B eher die flexible Organisation von Regeln, Rollen, Abläufen und Kommunikationstechnologien zwischen Softwaresystemen im Vordergrund.

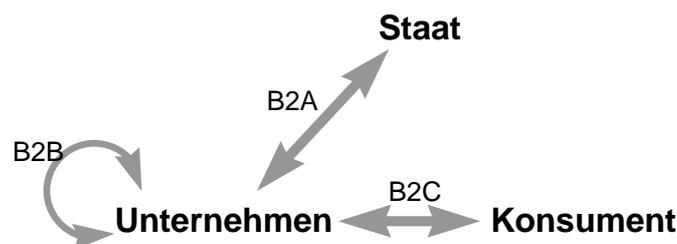


Abb. 1: Geschäftsbeziehungen und beteiligte Rollen

2.2.1.1 Business-to-Business

B2B-Commerce findet zwischen Unternehmen statt. Dabei muß man sich vergegenwärtigen, daß Handel nicht zwischen einer Gruppe von Anbietern und einer von Nachfragern stattfindet, sondern entlang komplexer Wertschöpfungsketten. Je nach Markt tritt ein Unternehmen dann in der Rolle des Anbieters oder Nachfragers auf. B2B-Commerce bedeutet zunächst, daß überhaupt „Handel“ zwischen Unternehmen stattfindet. Dies ist heute nicht immer der Fall: wenn ein Zulieferer z.B. mit einem Automobilhersteller über mehrere Jahre einen Rahmenvertrag schließt, so findet „Handel“ nur einmal statt, der Rest ist Abwicklung, Kommunikation, Transport. B2B-Commerce hilft, den Handel bei der Kooperation zwischen Unternehmen in den Vordergrund zu stellen. Dabei kann es zum einen eine Rationalisierung der herkömmlichen Herangehensweise sein oder aber auch die Schaffung von Verfahren, mit denen neuartige „Business Models“ realisiert werden können.

B2B wird im wesentlichen durch Softwaresysteme unterstützt. Der Mensch tritt dabei eher in der Rolle des Konfigurators auf. In Ausnahmefällen kann auch eine Entscheidung, die nicht im Regelwerk der Software verankert werden kann, durch den Menschen gefällt werden.

Typische aktuelle Anwendungen im B2B-Bereich sind Auktionssysteme (Beschaffung und Vertrieb), Broker-Systeme zur Zusammenführung von Anbietern und Nachfragern, Handelssysteme (die den Handel von Gütern mit einfacher Produktspezifikation unterstützen) sowie letztlich jede Form von Extranet-Integration zwischen Unternehmen (für den Austausch von Vertriebsinformation, Preislisten, AGBs etc.).

Extranets dienen dabei als Kooperationsgrundlage zwischen Geschäftspartnern, die sich gegenseitig Zutritt zu einem Teil ihrer Daten und Online-Dienstleistungen verschaffen (siehe Kapitel XXX). Traditionell werden Value-Added-Networking-Dienste eingesetzt, um Geschäftsnachrichten auszutauschen. Hierbei stand bisher der elektronische Datenaustausch (EDI) im Vordergrund. Seit der Verbreitung des Internet stehen jedoch neuere Technologien wie WWW, CORBA und der XML-basierte Datenaustausch als Kandidaten zur Ablösung des EDI bereit (siehe Kapitel XXX). Extranet- und WWW-Anwendungen werden heute von einzelnen Unternehmen in proprietärer Form vorangetrieben. Daher ist der B2B-Bereich noch durch eine Fragmentierung von Märkten und individuellen Kooperationen charakterisiert. Eine mangelnde Standardisierung und Ad-hoc-Nutzbarkeit von Geschäftsprozessen hindert viele Unternehmen aufgrund der damit verbundenen Kosten. Zusätzlich ist auch der B2B-Bereich durch Rechtunsicherheit bei Abschlüssen von Online-Verträgen charakterisiert: 59% aller Umfrageteilnehmer sahen erhebliche Kosten im Bereich von online-Vertragsabschlüssen (vgl. EU-Studie [EU98]).

Als Beispiele lasse sich die im Vorwort erwähnten Szenarien zum Data-Mining, zum Online-Notar oder auch das Thema der Business Objects nennen.

2.2.1.2 Business-to-Consumer

Beim B2C-Commerce steht vor allem der Bestell- und Verkaufsprozeß eines Anbieters gegenüber einer großen, wechselnden Zahl an Kunden im Vordergrund. Zumeist ist das Transaktionsvolumen niedrig und die Bindung zwischen den Handelspartnern eher locker. Als Kunde tritt zumeist eine einzelne Person auf. Folglich sind EC-Systeme für den B2C-Bereich Web-basierte Katalog- und Buchungsanwendungen, mit deren Hilfe die interaktive Suche nach Produkten unterstützt wird.

Der wesentliche Unterschied zum B2B-Commerce ist das Fehlen entsprechender Anwendungssoftware auf der Kundenseite (nur Web-Browser) und die Konfiguration einer Handelsbeziehung nach den individuellen Handelspraktiken der beteiligten Unternehmen. Natürlich kommt es auch zu Berührungspunkten zum B2B-Commerce, und zwar gerade dann, wenn ein Unternehmen sporadisch durch Browsing ein B2C-System (z.B. einen Online-Shop) benutzt. Dies ist der Fall, wenn Mitarbeiter Bücher bei Amazon..Com bestellen oder wenn Büroartikel individuell beschafft werden.

Der B2C-Bereich ist durch eher niedrige Transaktionsvolumen bis ca. 250 Euro charakterisiert und Transaktionen werden kurzfristig abgeschlossen, d.h. Bezahlung und Lieferung werden unmittelbar nach der Buchung eingeleitet. Im B2B-Bereich dominiert somit die Abwicklungsphase nach dem Transaktionsphasenmodell. Die Informationsphase wird bestenfalls durch Suchmaschinen und das Browsen des Käufers bei unterschiedlichen Anbietern unterstützt. Eine Verhandlung findet üblicherweise nicht statt, das individuelle Aushandeln zum Beispiel eines Rabattes würde für bei Amazon untragbare Personalkosten verursachen.

Von erheblicher Bedeutung ist beim B2C bereits heute der Umgang mit Kundendaten. Etliche Anwendungen konzentrieren sich inzwischen auf Möglichkeiten, Marketing- und Vertriebsinformationen aus Profilen herauszuxtrahieren. In engem Zusammenhang stehen Fragen des Datenschutzes, Verbraucherschutzes, der Vertragsabschlüsse über das Internet (entspricht dies der „Haustür“?) sowie regulatorische Rahmenbedingungen für den Web-Auftritt eines Anbieters. Nach einer Studie der EU-Kommission haben die Kosten der juristischen Beratung von Online-Anbietern aufgrund der Rechtsunsicherheit Regionen von 50 Stunden pro Monat und 35.000 Euro im Jahr erreicht [EU98]. Das gleiche gilt im übrigen auch für Unternehmen, die im B2B-Bereich über Extranets

Handel treiben.

Zum B2C-Bereich lassen sich die im Vorwort genannten Beispiele des virtuellen Supermarktes, des privaten elektronischen Geldes sowie zum Datenschutz nennen.

2.2.1.3 Administration-to-Business

Der Staat (bzw. die öffentliche Verwaltung) ist verpflichtet, gewisse Beschaffungsmaßnahmen nach einem vorgegebenen Ausschreibungsmuster durchzuführen. Bei einer öffentlichen Ausschreibung werden Aufträge in Form von Leistungsbeschreibungen spezifiziert und publiziert. Innerhalb gegebener Fristen können Unternehmen nun Angebote unterbreiten, die nach vorgegebenen Kriterien zu vergleichen und bewerten sind. Diese Prozedur läßt sich durchaus automatisieren, indem Publikations- und Einreichungskanäle durch entsprechende EC-Software realisiert werden.

A2B-Commerce ist somit heute sehr stark am Beschaffungswesen orientiert und beschränkt sich damit zumeist auf die Unterstützung der Informations- und Verhandlungsphase. Die Ausführung ist im Bereich der Ausschreibung sowohl bez. der Prozedur als auch hinsichtlich der Produktspezifikation zu komplex, um automatisiert zu werden.

Grundsätzlich lassen sich A2B-Verfahren auch zwischen Unternehmen einsetzen: Das Beschaffungsvolumen großer Banken liegt beispielsweise im Bereich mehrerer Milliarden Euro. Durch den Einsatz von System zur Beschaffungsabwicklung können diese Kosten um ca. 5% gesenkt werden. Ein solches Beschaffungssystem zentralisiert im Innenverhältnis die Sammlung von Einzelanforderungen aus Geschäftsbereichen und Filialen und verhandelt im Außenverhältnis aufgrund des Volumens Lieferantenrabatte. Schon vor geraumer Zeit hat z.B. General Electrics (eines des größten und rentabelsten Unternehmen in den USA) einen wichtigen Teil ihrer EDI-Funktionalität – dabei insbesondere den Einkauf – auf WWW umgestellt: Dieser Umsatz über das Internet lag 1998 bei einer Milliarde Dollar. Die Kostenersparnis wird mit 5-20 % beziffert, da keine kostspielige EDI-Anbindung über proprietäre Netze nötig ist und da das Unternehmen damit die globale Konkurrenz unter den Lieferanten besser ausnutzen kann (denn nur zu den eher „teuren“ Anbietern konnten vorher Handelsbeziehungen per EDI aufgebaut werden).

2.2.1.4 Administration-to-Consumer

Es ist durchaus sinnvoll, Kunden über das Internet den Zugang zur öffentlichen Verwaltung zu ermöglichen (für elektronische Steuererklärungen, zur Arbeitsvermittlung etc.). Dennoch hat die A2C-Beziehung wenig kommerziellen Charakter. Der Staat hat seinen individuellen Bürgern wenig zu „verkaufen“, und das gleiche gilt umgekehrt. Jenseits des „Commerce“ sind allerdings hochinteressante Anwendungen denkbar, die auf neuen Internet-Technologien beruhen, wie z.B. die elektronische Steuererklärung (als Anwendung elektronischer Signaturen), Broker-Anwendungen zur Vermittlung Arbeitsloser, Mechanismen zur Bürgerbeteiligung (elektronische Wahlen, marktbasierter Prognose-Techniken etc.).

2.2.1.5 Administration-to-Administration

Zwischen Staaten findet ebenfalls kaum „Handel“ in einer Form statt, die durch EC-Systeme unterstützt werden könnte. Denkbar wären höchstens Auktionssysteme, über die Rechte erworben werden können – beispielsweise zur Emission gewisser Mengen von Kohlendioxid, den Einschlag von Tropenholz, FCKWs oder Walfangquoten. Aber auch die Integration von Zollbehörden und anderen öffentlichen Einrichtungen hilft, diese im B2A-Commerce als eine integrierte Einheit auftreten zu lassen. Bei den letzteren Beispielen findet jedoch kein originärer Handel zwischen öffentlichen Verwaltungen statt. Stattdessen nehmen etwa Zollämter eine unterstützende Funktion des internationalen B2B-Handels wahr.

2.2.1.6 Consumer-to-Consumer

Setzt man ein Szenario voraus, bei dem die gesamte Bevölkerung über einen Internet-Zugang und Möglichkeiten zur effizienten Online-Bezahlung verfügt, ist es nur natürlich, daß Privatpersonen im Internet Handel direkt treiben. Dies kann weit über Online-Dienste für den Autohandel oder zur Wohnungsvermittlung hinausgehen. Stellt man sich vor, daß alle denkbaren Soft-Goods, wie Musikaufnahmen, Urlaubsvideos, Gedichte oder Lösungen für Mathematik-Klausuren, handelbar werden, kann man annehmen, daß ein beträchtliches Volumen in diesem Segment erreicht werden kann. Wenn weltweit 100 Mio. Verbraucher durch unmittelbaren C2C-Handel jeweils nur 100 Euro jährlich ausgeben, ist bereits ein Volumen erreicht, bei dem es sich lohnt, über spezielle Systeme zur Unterstützung des C2C-Marktes nachzudenken.

So richtig spannend wird es jedoch erst, wenn geschlossene Benutzergruppen entstehen, die Handel treiben kön-

nen, ohne daß offizielles Geld fließt. Dies mag konspirativ klingen, ist jedoch recht banal. Nehmen wir an, T-Online hat im Jahre 2005 20 Mio. Mitglieder (da die Telekom die monatlichen Gebühren weiterhin drastisch gesenkt hat ;-). Was wäre, wenn innerhalb dieser Gruppe der T-Taler als Verrechnungseinheit eingesetzt werden könnte? Dann „tauschen“ alle Teilnehmer Dienste, Waren und T-Taler gegeneinander aus, ohne daß am Ende auch nur eine DM Steuern anfallen. Warum? Weil die Telekom den Umlauf von T-Talern als Kundenbindungsinstrument einsetzt, ohne bei jeder Transaktion einen Obulus zu verlangen. Dazu mehr in den späteren Kapiteln.

Im begrenzten Rahmen wird bereits heute C2C-Commerce getrieben, indem beispielsweise Privatanwender für sich gegenseitig Werbung treiben (Bannertauschringe) oder in dem so etwas wie Nachbarschaftshilfe mit einem Bonussystem online realisiert wird.

2.2.1.7 Zusammenfassung

Natürlich verwischen die Grenzen zwischen diesen Kategorien regelmäßig. Beispielsweise treten auch Unternehmen als Consumer-artige Kunden auf, wenn sie beim Zulieferer Bleistifte anhand dessen Web-Katalog bestellen. Umgekehrt kann eine Einzelperson als Anbieter eines professionellen Dienstes auftreten, wie z.B. ein Taxifahrer oder Übersetzer. Schließlich sind entsprechende Anbieter/Nachfrager-Beziehungen auch innerhalb einer Organisation anzutreffen – zum Beispiel dann, wenn eine Einkaufsabteilung für die anderen die Beschaffung zentralisiert und durchführt. Ist diese als Profit-Center organisiert, steht sie in unmittelbarem Wettbewerb mit externen Zulieferern.

Folglich muß man auf die tatsächlich eingesetzten Mechanismen und Verfahrensregeln achten, wenn man B2B von B2C differenzieren will:

Häufig verbleibt als Unterscheidungskriterium zwischen B2B und B2C nur noch die Tatsache, daß beim B2B ein höherer Automatisierungsgrad als beim B2C vorherrscht. Während im letzteren Fall eher der Benutzer am Web-Browser als “Consumer“ im Vordergrund steht, trifft man beim B2B miteinander kommunizierende, integrierte Softwareprozesse an (vgl. auch Abschnitt XXX).

Aufgrund dieser Konfusion soll im folgenden das Transaktionsphasenmodell zur Klassifikation herangezogen werden.

2.2.2 Phasen der Handelstransaktion

Jede kommerzielle Handelstransaktion, die über organisatorische Grenzen hinweg durchgeführt wird, führt direkt oder indirekt zu einem Vertrag, der zwischen den beteiligten Parteien geschlossen wird. Dieser Vertrag hält deren Verpflichtungen fest, die dort definierten Leistungen zu erfüllen. Gleichzeitig definiert er die jeweiligen Rechte, die den anderen Parteien daraus erwachsen. Die austauschbaren Leistungen sind dabei Dienste, Güter, Rechte oder Zahlungen.

In der Literatur werden für eine derartige Transaktion drei Phasen unterschieden [Schm95]:

- In der *Informationsphase* beobachten Teilnehmer den Markt und unterbreiten möglichen Partnern Angebote. Während der Produktsuche werden dabei Produktspezifikationen - also Preise, Qualitätsmerkmale etc. - zur Evaluation herangezogen.
- In der *Verhandlungsphase* treten potentielle Partner zunächst in Verbindung, um über Angebote und Gegenangebote diese Spezifikationen iterativ anzupassen. Dieser Verhandlungsprozeß führt entweder zu einem Zustand der Einigung oder er wird abgebrochen.
- Schließlich stellt die Vertragsunterzeichnung den Übergang dar zur *Abwicklungsphase*. Diese Phase kann zeitlich zwischen wenigen Sekunden und mehreren Jahren dauern.

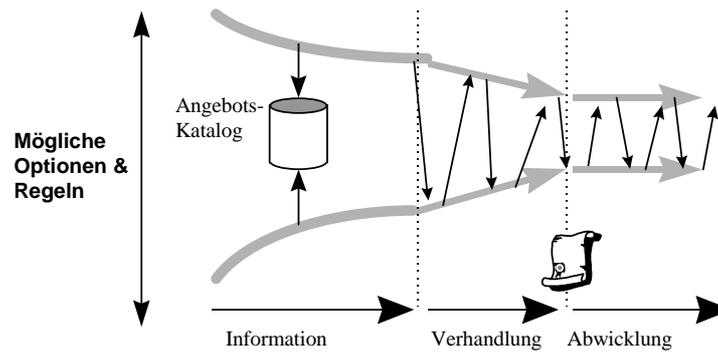


Abb. 2: Phasen einer Handelstransaktion

2.2.3 Transaktionsvolumen

Gerade im B2C-Bereich werden Transaktionen häufig nach ihrem Volumen unterschieden. Dies erfolgt nicht willkürlich, sondern insbesondere wegen der damit verbundenen unterschiedlichen Geschäftsmodelle und technischen Verfahren der Zahlungsabwicklung. Es besteht keine allgemeine Einigkeit über die Grenzwerte zwischen den unterschiedlichen Ausprägungen dieser Klassifikation. Folgendes Schema kommt der "herrschenden Meinung" wohl am nächsten:

- Nanopayments (0,01 – 0,2 Euro)
- Micropayments (0,1 – 5 Euro)
- Medium Payments (5-1.000 Euro)
- Makropayments (≥ 1.000 Euro)

Diese Aufteilung orientiert sich stark an den zugrundeliegenden Geschäftsbeziehungen und den dafür eingesetzten Zahlungsverfahren.

Dabei wird angenommen, daß bei **Macropayments** eine wohletablierte Beziehung zwischen den Transaktionspartnern existiert. Es handelt sich beispielsweise um den internationalen Kauf und Transport einer Ladung PCs oder ein Softwareprojekt. Hierbei tritt die Abwicklung der Zahlungstransaktion hinter diversen anderen Vereinbarungsprozessen zurück. Insbesondere steht die Vertrauensbildung zwischen Personen im Vordergrund. Aufgrund des Volumens sind die hohen Transaktionskosten internationaler Akkreditivgeschäfte tolerierbar und können nur schwer durch Internet-Zahlungsverfahren ersetzt werden.

Medium Payments liegen in dem Bereich, der heute durch Kreditkarten und Schecks abgedeckt werden kann. Es ist keine etablierte Vertrauensbeziehung auf persönlicher Ebene erforderlich, vielmehr werden Dritte als Vertrauensträger involviert (Banken, Kreditkartengesellschaften). Diese Zahlungsverfahren haben die größten Chancen, das Standardinstrument zur Bezahlung im Internet zu werden. Dies liegt nicht nur an der bereits heute befriedigend gelösten technischen Umsetzung mit Unterstützung verschiedener kryptographischer Verfahren, sondern auch an der einfachen Übertragbarkeit der Vertrauensverhältnisse: Es ist die Kreditkartengesellschaft, die dem Händler mitteilt, daß ein Kunde finanziell in der Lage ist, eine Zahlung durchzuführen. Gerade in diesem Segment spielen vertrauenswürdige Dritte aus dem Finanzsektor eine tragende Rolle.

Bei **Micropayments** sieht die Situation anders aus. Hier bleibt in der klassischen Welt nur das Bargeld als Zahlungsmittel. Es ist flexibel handhabbar, und es ist keine Bank zur Verifikation erforderlich, wenn der Kunde auf dem Flohmarkt als Wechselgeld 27 Pfennige erhält. Bereits die hier genannten Eigenschaften – Offline-Nutzung, Teilbarkeit und Anonymität – sind nach bisherigen Erfahrungen für viele Verfahren bereits KO-Kriterien für die Internet-Umsetzung als "Elektronisches Geld" (siehe auch Abschnitt XXX). Dennoch wäre es schade, wenn sich die Lücke der Micropayments zwischen etwa 0,1 und 5 Euro nicht schließen ließe; gerade hier würden interessante Geschäftsmodelle im B2C- oder C2C-Commerce ausgeschlossen werden.

Am unteren Ende der Skala liegen **Nanopayments**. Diese Bezeichnung sollte man einführen, damit ein Segment benennbar wird, für das sich der Aufwand eines Micropayment-Verfahrens definitiv für niemanden rechnet. Hier gibt es zwei Lösungen: entweder werden Güter ohne Bezahlung abgegeben – das Geschäftsmodell sieht hier andere Einnahmequellen wie Banner-Werbung vor – oder es werden Verfahren eingesetzt, die so leichtgewichtig sind, daß sie nicht durch komplexe Kommunikation und kryptographische Verfahren gebremst werden. Ferner

sind diese Beträge so niedrig, daß auch das Vertrauen in die Beteiligten nicht dem in Banken oder Kreditkartengesellschaften entsprechen muß.

Electronic Commerce ist auf allen Ebenen realisierbar. Wichtig ist jedoch festzustellen, daß im Bereich der Micro- und Nanopayments die Geschäftsmodelle immer spekulativer – und damit vielleicht auch interessanter – werden.

2.2.4 Anwendungsnähe der EC-Technologie

Unabhängig vom Phasenmodell stellt die Anwendungsnähe einer EC-Technologie eine zweite Dimension dar, bei der eine Klassifikation nach *architekturellen Ebenen* vorgenommen werden kann:

- **Basisdienste / “Enabling Technologies“.** Diese realisieren spezifische Funktionen und Mechanismen wie z.B. SmartCards, Kommunikationsprotokolle, Verschlüsselungsalgorithmen etc. Basisdienste sind an sich nicht auf den EC-Einsatz beschränkt.
- **EC-Middleware.** Als “Middleware“ bezeichnet man Plattformen, die einen Werkzeugkasten aus kombinierbaren Komponenten und Technologien zur Verfügung stellen. Diese sind jedoch ohne weiteres noch nicht für einen bestimmten Anwendungszweck einsetzbar. Middleware implementiert also noch kein Anwendungswissen. Als Beispiele seien CORBA, Java, Public-Key-Infrastrukturen etc. genannt. Auch “EC-Middleware“ ist nicht auf den EC-Anwendungsbereich beschränkt, vielmehr kann man darunter alle Middleware-Systeme verstehen, die für den Bereich Electronic Commerce eingesetzt werden können. Im Gegensatz zum Basisdienst zeichnet sich Middleware durch die Kombinierbarkeit seiner Bestandteile aus: CORBA verdeckt die Heterogenität seiner Implementierungen durch eine einheitliche Abbildung auf gemeinsame Protokolle und Schnittstellenkonventionen. Gleiches gilt für DCE oder reine Java-Middleware.
- **EC-Frameworks.** Ein EC-Framework faßt verschiedene Middleware-Komponenten zusammen. Im Gegensatz zur Anwendung bietet das Framework jedoch ein Gerüst für den Softwareentwickler, das Prozesse, Datenstrukturen und Schnittstellen vorgibt. Für eine spezifische Anwendung kann der Programmierer das Rahmenwerk mit Leben füllen. Frameworks sind eine relativ junge Technologie, um komplexe Softwaresysteme beherrschbar zu machen. Gerade im Bereich des EC sind sie jedoch besonders vorteilhaft: grundlegende Strukturen lassen sich vom Anbieter des Frameworks vordefinieren, so daß der Anwender sich nur noch mit individuellen Erweiterungen auseinandersetzen muß. Ein Produkt, das diesem Ansatz folgt, ist das San Francisco-Framework der IBM, das in Kapitel XXX beschrieben wird.
- **EC-Anwendungen.** EC-Anwendungen sind spezifisch für eine bestimmte Branche oder Funktion innerhalb des Transaktionsprozesses. Beispiele sind Auktionssysteme, Online-Kataloge etc. Durch eine geeignete Parametrisierung lassen sich Anwendungssysteme für unterschiedliche Branchen, Produkte oder Handelsprozesse einsetzen. EC-Anwendungen werden jedoch nur durch den Administrator konfiguriert und nicht durch Programmierung. Eine Anwendung kann aus einem Framework heraus entwickelt werden: Dabei ist dies z.B. für Auktionssysteme denkbar, deren Grundfunktion vorgegeben ist; lediglich der Auktionstyp ist durch Vervollständigung des Gerüsts noch zu implementieren.

Alle denkbaren Aspekte des Electronic Commerce lassen sich mehr oder weniger präzise den Transaktionsphasen sowie den architekturellen Ebenen zuordnen:

Tabelle XXX: Einordnung verschiedener Electronic-Commerce-Technologien

	Informationsphase	Verhandlungsphase	Abwicklungsphase	Weitere Klassifikation
EDI	Kataloge	EDI-Rahmenvertrag	EDI-Nachrichten	B2B, Makro
El. Zahlungsverfahren		JEPI, Wallets	Zahlungstransfer	B2C, Mikro-Makro
Banner-Werbung	Im Web			B2C, B2BC
Virtuelle Unternehmen	Profile, Angebote	El. Contracting Integrierte Marktplatzsysteme	Workflow Management	B2B

Shopping Malls	Produktkataloge und Metainformation		Wallets & Payment Gateways	B2C, B2BC, Mikro-Makro
Brokerage		Integrierte Marktplatzsysteme		B2B
SmartCards		Authentisierung	Bezahlung	B2C, B2B
Workflow-Mgmt			Abwicklung Interorg. Geschäftsprozesse	B2B
Electronic Contracting	Bereitstellung von Vertragsformularen	Vertragsverhandlung und -abschluß	Kontrollierte Vertragsausführung	B2B, B2C
Agentensysteme	Schaffung von Markttransparenz	Verhandlungsprotokolle und -strategien	Durchführung von Käufen	B2B, B2C
Business Objects	Eintragung in Kataloge	Verbindliche Objekt-Konfiguration	Ausführung von Methodenaufrufen	B2B

3 Electronic Commerce und die Statistik

Dieses Vorab...

Kein EC-Buch, kein Artikel, kein Vortrag, der nicht die üblichen Wachstumsprognosen und Statistiken zum Thema EC zitiert. Dabei wissen wir alle, daß diese Statistiken nicht nur aufgrund ihrer *empirischen Basis*, sondern auch wegen *diffuser Definitionen und Abgrenzungen* sowie nicht zuletzt wegen der *inhärenten Dynamik* dieses Themas nur ganz allgemeine Aussagen im Sinne von Allgemeinplätzen machen können:

Zur empirischen Basis: Einige der bekannten Prognosen aus dem Jahre 1996 (Forrester, Ovum) fußen auf einem Beobachtungszeitraum von 2-3 Jahren, d.h., aus dieser Historie auf ein Volumen von 500-1.000 Mrd. USD zu schließen, ist ein wenig gewagt. Andererseits ist durchaus nicht zu bestreiten, daß dieses Volumen erreicht werden kann – es besteht nur meist keine Information darüber, welche technische Infrastruktur diesem sog. EC zugrunde gelegt wird:

Zur Definition und Abgrenzung: Ist es bereits EC, wenn ein Geschäft per e-Mail abgeschlossen wird? Damit wären die Seminare, die ich veranstalte, bereits ein Mosaiksteinchen im EC-Marktvolumen, da diese zumeist per e-Mail vereinbart und abgeschlossen werden. Wie sieht es aus beim Fax? Ein erheblicher Teil aller volkswirtschaftlichen Wirtschaftstransaktionen wird per Fax abgeschlossen. Wenn nun Fax (oder gar Telefonie!) über das Internet abgewickelt wird, ist dies dann EC? Wie sieht es aus mit EC über VANS? Dieser findet bereits seit einigen Jahren statt (EDI), wird jedoch von einigen Statistiken nicht erfaßt. Eine Migration in Richtung Internet hätte somit lediglich Substitutionscharakter. Es hängt also ganz eindeutig von der architekturellen Abgrenzung ab, welches Medium als EC-relevant hervorgehoben werden kann. Basisdienste und „Enabling Technologies“ fallen hier definitiv heraus. Folglich sollten nur Handelstransaktionen berücksichtigt werden, die eindeutig über EC-Systeme abgewickelt werden.

Zur Inhärenten Dynamik: Für das Internet lassen sich nicht immer technische oder ökonomische Pauschalurteile treffen. Noch nie zuvor war die Hebelwirkung einer neuen Technologie größer als im Internet. Web-Browser und -Server haben binnen weniger Jahre die Art und Weise, sich zu informieren, zu kaufen und zu kooperieren, vollständig verändert. Niemand konnte dies im Jahre 1993, als die ersten Browser in akademischen Kreisen entwickelt wurden, vorhersagen. Umgekehrt wurde der Push-Technologie etwa im Jahre 1995 eine ähnliche Entwicklung vorhergesagt. Unternehmen wie CastaNet, die Push-orientierte Java-Middleware zu entwickeln ankündigte, wurden heiß gehandelt. Dennoch besitzt „Push“ heute ein kommerziell eher irrelevantes Volumen. Ähnliches gilt für Technologien wie intelligente oder mobile Agenten: So „appealing“ diese Technologie sein mag, das „Marktvolumen“ läßt sich heute immer noch lediglich in der Zahl der akademischen Veröffentlichungen messen. Ganz anders sieht es hingegen z.B. in speziellen Branchen wie dem Internet-Banking aus. Unternehmen wie etwa Brokat entwickelten zum richtigen Zeitpunkt die richtige Software für den Markt der Finanzdienstleister, so daß dort binnen weniger Jahre über 600 europäische Banken Internet-fähig gemacht werden konnten. Ein Wachstum, auf das weniger durch irgendeine Extrapolation historischer Daten geschlossen werden kann, sondern das insbesondere von der geschäftlichen Cleverness und den technischen Finessen einer Produktinnovation abhängt. Hätte man das Wachstum im Bereich der PDAs bis 1997 aus dem des Apple Newton hochgerechnet, würde man sicherlich für das Jahr 2005 ein anderes Volumen errechnen als zum heutigen Zeitpunkt, zu dem sich durch neue Produkte (Palm Pilot, Windows CE, Satellitennavigation etc.) die Perspektiven drastisch geändert haben.

Also: Wachstum findet heute eher qualitativ als quantitativ statt. Anstelle das Volumen *eines* Marktes zu messen (und dabei eventuelle Nachbar- oder Offspring-Märkte aus den Augen zu verlieren), gilt es heute eher, die „Geburtenrate“ zukünftiger, neuer Märkte zu schätzen. Da dies von Faktoren wie politischer Regulation, ökonomischen Rahmenbedingungen, wie z.B. Netzzugangskosten, der Ausbildung und Risikobereitschaft einer Gesellschaft und letztlich von der Entwicklung der technologischen Infrastruktur, abhängt, sind heute entweder auf der Makroebene nur aggregierte Großschätzungen erlaubt oder auf der Mikroebene das Kreieren eines Marktes, von dem der Statistiker oder Analyst erst in einem Jahr erfahren wird.

Dazu noch ein Beispiel: Im März 1996 hatte ich ein Gespräch mit einem EDV-Leiter eines Hamburger Verlags-hauses. Die Frage war, wann sich elektronisches Geld in Deutschland durchsetzen würde. Er ging von sechs Monaten aus, da Unternehmen sich bereits dieser Sache angenommen hatten (damals war die Deutsche Bank bereits mitten in der Vorbereitung ihres eCash-Feldtests). Dem war zu entgegenen, daß eCash technologisch bereits seit vielen Jahren möglich gewesen sei und daß das eigentliche Problem jedoch in der organisatorischen Umsetzung läge. Heute wissen wir, daß trotz der internationalen Begeisterung für eCash seitens der Verbraucher, einiger Banken sowie sogar der Notenbanken (die es zumindest nicht grundsätzlich ablehnen) dieses Verfahren bislang erfolglos war.

Und jetzt ein Beispiel, das aus heutiger Sicht (März 1999) einen ähnlich unwägbareren Ausgang nehmen kann: Die Geldkarte (siehe auch Kapitel XXX). Obwohl sie über 45 Millionen Benutzern zur Verfügung steht, wird sie nicht einmal von 500.000 genutzt. Zu erwarten ist, daß sich auch andere Kartensysteme (Mondex und kreditkartenbasierte Verfahren) ihren Marktanteil in Deutschland zu erkämpfen suchen. Jetzt die Frage an den Marktforscher: entspricht die Geldkarte eher dem eCash oder dem WWW? Wird dieser Markt explodieren und neue Add-on-Produkte generieren? Oder wird man feststellen, daß sich das Business-Modell „Geldkarte“ eigentlich gar nicht rechnet, weil es für irgend jemanden der Beteiligten zu teuer sein könnte? Dieser Markt steht und fällt insgesamt mit der Cleverness derer, die ihn heute vorbereiten, derer, die ihn regulieren, der tolerierten Unsicherheit und dem langen Atem derer, die Anfangsinvestitionen zu tragen haben. Anerkennung gilt dem Analysten, der diese und mir selbst unbekanntere Faktoren kennt, sie richtig gewichtet und dann auch noch korrekt quantifiziert und extrapoliert.

Dies also vorweg. Wenden wir uns nun dem Zahlenmaterial zu. Eine fast unerschöpfliche Quelle, die im Gegensatz zu einem Buch auch weiterhin (hoffentlich) aktuell bleiben wird, ist das „Projekt 2000“ der Vanderbilt University (www2000.ogsm.vanderbilt.edu). Also bitte spätestens 6 Monate nach Erscheinung dieses Buches die folgenden Zahlen überprüfen ;-)

3.1.1 Demographisches aus der Internet-Gemeinde

■ Allgemeine Online-Statistiken: <http://www.cyberatlas.com>

■ Online Auktionen: http://www.moai.com/landing_internet_ad1.html

Mehr als 50 Millionen US-Bürger besitzen einen Internet-Zugang, dabei verdoppelte sich diese Zahl bisher alle 18 Monate [AdYe98]. Es ist allerdings zu erwarten, daß sich dieses Wachstum bei einer Durchdringung von mehr als 40% sehr bald abflachen wird. Dennoch wird sich laut Ovum die Internet-Bevölkerung bis zum Jahr 2005 vervierfachen (Ovum-Report "Internet Market Forecasts: Global Internet Growth 1998-2005", Dez. 1998, http://www.cyberatlas.com/big_picture/demographics/ovum.html). Damit werden 2005 206 Millionen Einwahlverbindungen und 17,5 Millionen Festverbindungen vorliegen. Im Gegensatz zu den USA werden Europa und Asien den Hauptanteil des Wachstum in den folgenden Jahren ausmachen. Der Computer-Almanach geht sogar von über 300 Millionen Online-Bürgern weltweit *im Jahr 2000* aus. Dabei wird folgende Verteilung prognostiziert (<http://www.c-i-a.com/>):

Die 15 Länder mit der höchsten Internet-Benutzerzahl im Jahr 2000

Rang	Land	Internet-Benutzer (in Millionen)
1	USA	132.3
2	Deutschland	22.9
3	Japan	21.9
4	Großbritannien	17.0
5	Frankreich	12.6
6	Kanada	11.6
7	Italien	10.6
8	Australien	8.0
9	Niederlande	5.4
10	Brasilien	5.2
11	Rußland	5.0
12	Spanien	4.4
13	China	3.8
14	Schweden	3.7
15	Südkorea	3.2
Top15Countries		267.5
Europe		102
Worldwide		327

Das Wachstum wird sich laut EITO [EITO99] etwas moderater vollziehen. Hier sind im Jahre 2001 ca. 68 Millionen Online-Benutzer zu erwarten. Dabei liegt das Verhältnis zwischen Geschäftskunden und Privatkunden bei 1:3.

Tabelle XXX: Entwicklung der Internet-Nutzung in Europa (1995–2001)

	1995	1996	1997	1998	1999	2000	2001
Geschäftliche Nutzer	6.466	10.679	13.898	14.269	14.676	15.660	16.547
Private Nutzer	5.860	10.027	12.641	19.637	28.502	39.063	51.224
Summe	12.326	20.706	26.539	33.906	43.183	54.723	67.771

70% aller US-PC-Besitzer surfen im Netz.

Jeder dritte US-„Netizen“ kauft auch online.

In Deutschland sind laut GfK 8,7 % der Bevölkerung online, in den USA laut Intelliquest 27,8 % (siehe NUA).

In Deutschland sind 12 Millionen Teilnehmer online, dies sind immerhin 15% der Bevölkerung. In Finnland befinden sich jedoch 1,43 Millionen Menschen und damit 28 Prozent der Bevölkerung online (37 Prozent der Erwachsenen) – dies ist die höchste nationale Durchdringung weltweit.

Europa und Deutschland

Aktuelle Informationen zur Internet-Host und DNS-Domänenstatistik finden sich beim RIPE Network Coordination Centre (www.ripe.net). RIPE ist der Europäische RIR (Regional Internet Registry) für Europa und benachbarte Regionen. Dabei werden Internet-Statistiken der LIRs (Local Internet Registry) der einzelnen Länder aggregiert. Hier finden sich die Rohdaten für Statistiken über die Anzahl von DNS-Domänen, die durchschnittliche Größe über das Web abgerufener Dateien, die Verteilung des Internet-Traffic pro Tag, Woche und Monat – und

dies tagesaktuell.

Laut EITO-Statistik wird sich die Anzahl der Web-Browser in Europa von 14,2 Millionen in 1997 auf 58 Millionen Ende 2001 erhöhen. Hierzu sind neben PC- und Workstation-basierten Browsers vor allem auch mobile und TV-basierte Systeme zu zählen. Die Anzahl aktiver Internet-Teilnehmer¹ wird sich im gleichen Zeitraum von 27 auf 68 Millionen erhöhen.

Interessante Informationen zur Web-Demographie in Deutschland liefern die W3B-Umfragen der Hamburger Marktforscher Fittkau & Maaß, die im Rahmen ihrer 6. Studie insgesamt 16 248 europäische WWW-Nutzer befragten. Im europäischen Vergleich ließen sich dabei erhebliche Unterschiede feststellen. Beispielsweise schwankt der Frauenanteil bei den Internet-Benutzern erheblich: in Belgien, Deutschland, Österreich, Luxemburg, Italien und der Schweiz liegt der Anteil bei 12-16 Prozent (Deutschland: 15,5%). In Skandinavien beginnt er hingegen bei 19 Prozent (Dänemark) und reicht bis über 36 Prozent (Norwegen, Schweden). Hoch ist der Frauenanteil ebenfalls in Frankreich (26%), Großbritannien (28%) sowie den Niederlanden und Spanien (über 36%).

Andere Studien relativieren diese Zahlen ein wenig; so zeigt ein Ergebnis der ARD/ZDF-Studie zu diesem Thema, daß 28% der deutschen Nutzer weiblich sind (<http://www.das-erste.de/studie/ardonl.pdf>).

XXX In Deutschland liegt das Durchschnittsalter bei 35,5 Jahren.

- > In der Begründung für den Entwurf unterstreicht die Kommission noch einmal
- > die wirtschaftliche Bedeutung der Wachstumsbranche. Bis zum Jahr 2000 soll
- > das elektronische Handelsvolumen weltweit 200 Mrd Ecu betragen.

Bildungsstand

Hier die wichtigsten demographischen Daten der deutschen Internet-Gemeinde aus dem Jahr 1998: Nach Fittkau & Maaß [XXX] besitzen 63,9% aller Internet-Nutzer das Abitur oder einen höheren Abschluß. Diese Zahl wird durch eine ARD/ZDF-Studie bestätigt (63%). Beruflich verteilt sich die Nutzergemeinde folgendermaßen:

Berufsgruppe	Anteil
Studenten	17,1
Angestellte	43,6
Selbständige	16,3
Schüler / Auszubildende	8,0
Doktoranden	2,4
Beamte	4,5
Sonstige	8,1

Quelle: **Fehler! Textmarke nicht definiert.** XXX

Ein etwas anderes Bild ergibt sich für den Bildungsstand der europäischen Internet-Nutzer, die im Rahmen der W3B-Studie befragt wurden. Abitur oder einen vergleichbaren Schulabschluß besitzen in den Niederlanden, der Schweiz, Dänemark und Österreich jeweils nur etwa 47 bis 58 Prozent. Im Mittelfeld liegen Deutschland, Belgien, Luxemburg und Norwegen, bei denen zwischen 63 und 65 Prozent einen dem Abitur vergleichbaren Abschluß besitzen. In Großbritannien/Irland, Schweden und Italien liegt der Anteil bei 71 bis 83 Prozent. Die französischen Web-Nutzer haben mit 94 Prozent den höchsten Bildungsstand. Hier beträgt der Anteil der Studenten 20 Prozent – dies ist der höchste in Europa, gefolgt von Österreich mit 18 Prozent. Ein Grund für den hohen französischen Anteil kann in der immer noch vorherrschenden Nutzung des Minitel-Systems liegen, das alle

¹ Teilnehmer, die ihren Account regelmäßig und nicht nur für e-Mail benutzen. Weitere Personen, die dieses Account mitbenutzen sind nicht erfaßt.

wesentlichen Informations- und Transaktionsangebote umfaßt. Nur wer aus beruflichen oder privaten Gründen international kommuniziert, müßte das vergleichsweise weniger populäre Internet verwenden.

Tabelle **XXX:** **Die** **wichtigsten** **Internet-Anwendungen**
(Mehrfachnennungen) möglich)

Prozent **Internet-Anwendung**

96,8	E-Mail
95,0	World Wide Web (WWW)
74,0	Dateitransfer (Programme herunterladen)
34,8	Newsgroups (Usenet)
31,9	Java, Java-Scripts
26,6	Chat (Online-Diskussionen)
21,3	Übertragung von Audio und Video
19,9	Internet-Telefon und -Fax
16,2	Digitale Signaturen (z.B. Verisign, RSA)
9,3	3D-Welten, Virtual Reality (VRML)
8,8	Video-Konferenzen via Internet
4,9	Push-Technologien/-Channels

Quelle: **Fehler!** **Textmarke** **nicht** **definiert.**

Nach der Studie von W3B wurden E-Mail und WWW von fast allen (95%) Teilnehmern verwendet. Java bzw. JavaScript wird lediglich von einem Drittel eingesetzt. Dabei ist jedoch fraglich, ob jeder Teilnehmer sich bewußt ist, wann immer ein Applet oder ein JavaScript ausgeführt wird. Relativ hoch erscheint die Nutzung von Audio/Video-Übertragungen. Auch hier ist unklar, ob es sich um aktive (Web-Cam) oder passive Nutzung (Player), bzw. in jedem Fall um Internet-Streaming-Anwendungen handelt. Erstaunlich ist der ebenfalls relativ hohe Anteil digitaler Signaturen. Auch hier ist allerdings fraglich, wie oft eine digitale Signatur wirklich in der täglichen Praxis genutzt wird und welchem Qualitätsstandard die entsprechende Zertifizierungsstelle entspricht. Wie bereits erwähnt, hat sich die Push-Technologie definitiv noch nicht gegenüber dem „Pull-Prinzip“ des WWW emanzipiert. Bedenkt man jedoch, daß Spam-Mails im Prinzip Push-Inhalte sind und daß sicherlich jeder Teilnehmer hin und wieder damit belästigt wird, so zeigt sich einmal mehr, wie stark Statistiken durch schwache Definitionen an Wert verlieren. In der Presse veröffentlichte Glossen werden dieser Anforderung an Präzision häufig nicht gerecht.

Nutzungsstatistik auf Anwendungsebene

Eine jährliche Studie der Burda Medienforschung (<http://www.tdwi.com>) beschäftigt sich mit der Nutzung von Online-Angeboten. Grundlage dieser Statistik sind alle Internet-Nutzer, die mindestens einen Online-Dienst mit Internet-Zugang verwenden – also etwa 7,1% der von dieser Studie erfaßten deutschen Wohnbevölkerung über 14 Jahre.

Nutzung der Online-Angebote in Prozent (Mehrfachnennungen möglich)

55,9	E-Mails versenden
33,8	Produkt- bzw. Dienstleistungsangebote von Firmen
33,6	Aktuelle Wirtschaftsinformationen
30,8	Shareware, Software auf PC laden
30,0	Fahrplan- oder Flugplanauskunft
27,7	Home-Banking
26,8	mit anderen chatten, Newsgroups
23,6	Veranstaltungskalender für Theater, Kino etc.
23,4	Reisebuchungen, Reservierungen, Last-Minute-Reisen
22,0	Nachrichten aus der Politik
21,0	Lokales/Nachrichten aus der Region
17,5	Online spielen mit anderen Nutzern/ dem Computer
17,3	Jobsuche, Stellen- oder Wohnungsmarkt, KFZ-Markt
17,3	Boulevard, Unterhaltungsangebote
17,3	Online-Shopping, Home-Shopping
7,8	Erotikangebote

Quelle: Burda Medienforschung

Bemerkenswert ist ein Ergebnis des Berichts von FIND/SVP (www.futurestudy.com), daß es bis zum Jahr 2000 mehr als 24 Millionen Telearbeiter allein in den USA geben wird – dies entspricht XXX% der beschäftigten Bevölkerung. Auch in Deutschland steigt die Zahl der Telearbeiter: XXX.

Electronic Commerce

Electronic Commerce findet heute statt. Abgesehen von einigen typischen Branchen, die frühzeitig das Internet nutzten (Buchhandel, Reisebuchungen, CDs, Computer), befindet sich die heutige Online-Wirtschaft im Wandel von der Marketing-Nutzung hin zum Verkaufen. Das Online-Verkaufen wird von allen mit großem Rationalisierungspotential eingeschätzt.

Yahoo führt über 500.000 Unternehmen in seinen Verzeichnissen, wöchentlich wächst diese Zahl um 6.000 neue. Über 5.000 Online-Malls sind im Web zu erreichen, eine der größten ist iMall (www.iMall.com) mit über 1.800 Shops und über 40 Millionen Hits pro Monat (Nov. 1998).

Einer Studie der Giga-Group vom 4. Januar 1999 zufolge sind nur 5% aller Online-Unternehmen profitabel (<http://www.gigaweb.com>). Dies wird sich auch nicht wesentlich bis weit in das Jahr 2000 hinein ändern. Der eigentliche Vorteil der Web-Präsenz wird nach wie vor zunächst in der Optimierung der Kundenbeziehung liegen.

"Electronic commerce will play an increasing role in business, but even the best-known startups aren't profitable yet and only a few Fortune 100 companies have profitable Internet commerce operations," heißt es seitens der Giga-Group. Erst wenn Markenartikler beginnen, einen signifikanten Teil ihres Vertriebs auf das Internet umzustellen, wird Electronic Commerce mit dem „Classic Commerce“ konkurrieren können. In der Zwischenzeit wird es nur eher kleinen und flexiblen Frühadoptern gelingen, mit Hilfe neuester Technologie profitabel im Netz zu verkaufen. Sobald jedoch große Markennamen im Netz aufgetreten sind, wird die Zeit der Start-Up-Unternehmen schwieriger werden. Nur durch das Besetzen neuer Marktplätze kann es dann Einsteigern gelingen, profitabel zu wirtschaften.

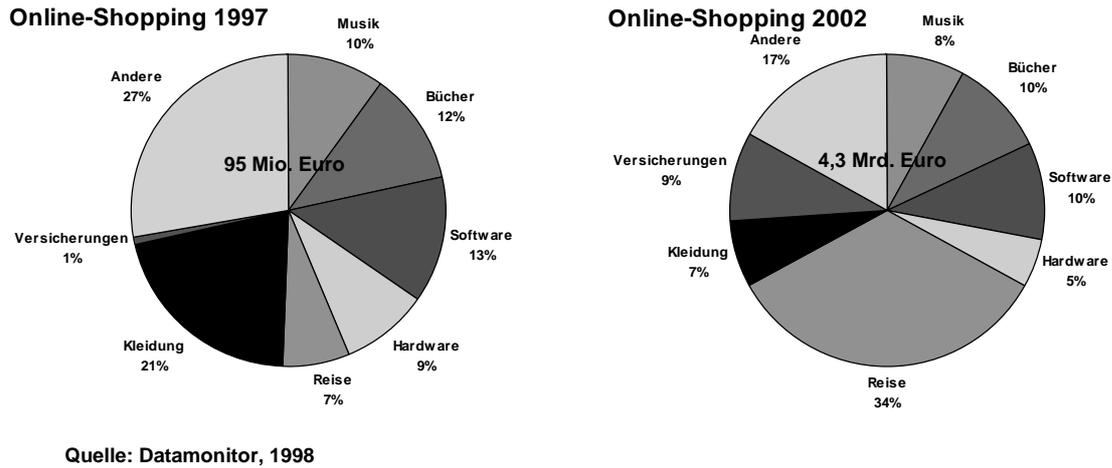
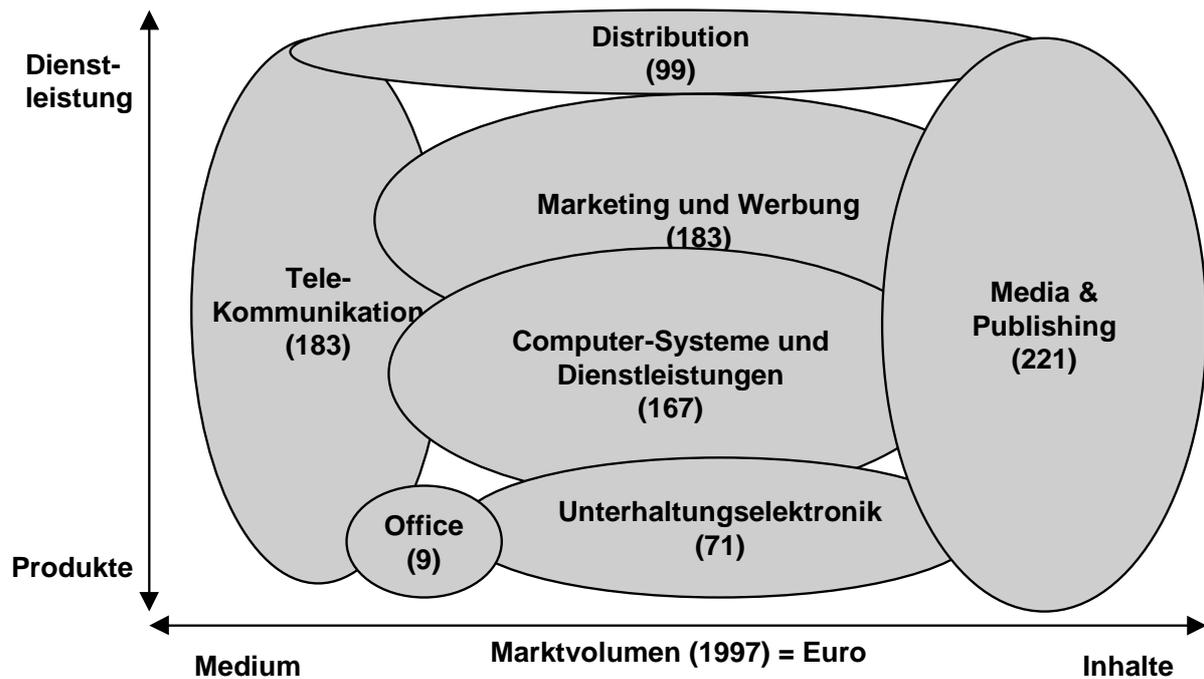


Abb. 3: Verteilung des B2C-Umsatzes 1997 und 2002

1998 prognostizierte IDC, daß EC-Umsätze im Bereich des Internet in Westeuropa² von 900 Millionen Euro im Jahre 1997 auf 26 Milliarden im Jahre 2001 steigen werden. Obwohl die beiden Haupthemmnisse „Jahr-2000“ und „Euro-Einführung“ Investitionen in den EC-Bereich nicht wesentlich beeinträchtigten, wird die Hauptwelle der Investition erst für die Jahre 2000 und 2001 erwartet. Dies liegt nicht zuletzt an einer eher abwartenden, weniger proaktiven Haltung der Entscheidungsträger. Ein weiterer Grund liegt im Mißtrauen in die Transaktions- und Rechtssicherheit von EC-Anwendungen insbesondere im B2C-Bereich.

40% aller Organisationen, die für eine Romtec-Studie [XXX] befragt wurden, gaben an, aufgrund des steigenden Wettbewerbdruk in EC zu investieren. Wenn ein Unternehmen mit seinem Warenangebot jedoch erst im Internet präsent ist, steigt der Wettbewerb weiter: Innovationen, die im Online-Angebot umgesetzt werden, können häufig binnen kürzester Zeit von der Konkurrenz kopiert werden. Häufig ist zudem heute noch ein Verbund unterschiedlicher Vertriebskanäle erforderlich, um Produkte auch über das Internet zu verkaufen. Dies liegt nicht zuletzt an der bis dato mangelnden Durchdringung des Internet sowie der gegebenen Intransparenz bzgl. des Warenangebots.

² EU, Schweiz und Norwegen



Quelle: [EITO99]

Abb. 4: Verteilung des Marktvolumen im Media/IT-Bereich 1997

- **Office:** Schreibmaschinen, Taschenrechner, Kopierer und andere Geräte
- **Unterhaltungselektronik:** Fernsehgeräte, Videorekorder, Radios, Kassettenrekorder, Uhren etc.
- **Media & Publishing:** Filme, TV-Programme, Videos, CDs, Schallplatten und Bänder.
- **Computersysteme und Dienstleistungen:** Hardware, Standardsoftware, Dienstleistungen.
- **Marketing und Werbung:** Online-Datenbanken, Online-Shops, Bestellkataloge, Werbung, Direktmarketing andere geschäftliche Dienstleistungen.
- **Distribution:** Rundfunk, Telex/Fax, Post, Paketversand, Kurierdienste.
- **Telekommunikation:** Telefonnetze, Datennetze, Kundengeräte, Dienstleistungsausrüstung, Installation & Wartung.

Kostenreduktion durch Electronic Commerce

Web-basierte Auftragsabwicklung. Die Verwendung eines Auftragsystems erlaubt im Internet die Prüfung des Lagerbestands eines Lieferanten, die Auftragserteilung sowie die Verfolgung der Produktion und Lieferung. US-Anbieter berichten der Giga-Studie zufolge von einer Reduktion der Kosten zur Auftragsbearbeitung von 8-25 USD auf 0,03-1 USD.

Inkasso. Es ist zu erwarten, daß in den USA 600-700 Millionen Rechnungen im Jahr 2000 elektronisch zugehen und beglichen werden. Durch die Reduktion von Druckkosten, Porto, Versandbearbeitung etc. ist eine Reduktion um 60-70% der Kosten zu erwarten.

Kundendienst. Hier wird zunächst nicht mit geringen Kostenreduktionen nach der Einführung einer Web-basierten Lösung gerechnet, sondern eher mit zusätzlichen Kosten durch den gleichzeitigen Betrieb einer Online- und Telefon-basierten Infrastruktur. Mittelfristig (nach etwa 3 Jahren) wird jedoch eine Reduktion um 10-40 Prozent erwartet.

XXX Es bleibt schwierig...

Zona Research zufolge scheitert ein Drittel aller potentiellen Kunden beim Versuch, Waren online zu bestellen. 62 Prozent gaben an, mindestens einmal bei der Suche nach einem Produkt aufgegeben zu haben.

„E-Commerce to Reach \$28 Billion This Year“

■ <http://www.internetnews.com/ec-news/>

Für Internet News, Inc. (<http://www.internetnews.com/ec-news/>) besteht der Elektronische Markt aus Internet, privaten Online-Diensten und CD-ROMs. In ihrer Studie wurde für das Jahr 1998 dafür ein Wachstum von 57,7% auf 28,2 Milliarden USD im Bereich B2C prognostiziert.

Davon entfallen 67,3% auf den Business-to-Business-Commerce (19 Mrd. USD). Für die weiteren Jahre bis 2002 liegt das jährliche Wachstum bei 30% und demzufolge bei 102 Milliarden USD. Der B2B-Commerce wird weiterhin den Löwenanteil einnehmen, jedoch stetig fallend (von 64,3% in 1999 auf 56,8 in 2002).

Als zweitgrößtes Marktsegment wurde der Bereich „Computer Products and Services“ identifiziert (23,6% in 1998 und 28,7% in 2002).

Nicht überraschend, liegt im B2C-Segment der Buchhandel an erster Stelle. Der US-Gesamtumsatz lag hier bei ca. 600 Millionen USD, 140% höher als 1997. Dieser Bereich soll bis 2002 auf 3,4 Milliarden USD anwachsen.

Zieht man den B2B-Bereich hinzu, lag der EC-Weltumsatz laut OECD 1996/1997 bei 26 Milliarden USD. Das Verhältnis aus B2B und B2C lag bei etwa 80:20. Dieser Studie zufolge könnte der EC auf bis zu 330 Mrd. USD in 2002/2003 und sogar auf 1 Billion USD im Jahre 2005 explodieren.

In Europa ist davon ist davon auszugehen, daß der Online-Handel Ende 2001 von 34% aller privaten und von 20% aller geschäftlich Internet-Teilnehmer genutzt wird.

In Deutschland

In Deutschland steht der Einzelhandel unter sehr hohem Wettbewerbsdruck. Seit fünf Jahren sinken die realen Umsätze dabei von 721,5 Mrd. DM in 1995 auf 715 Mrd. DM in 1997. Im Vergleich dazu fallen einige hundert Millionen Online-Umsatz kaum auf (ca. 0,2 bis 0,3 Prozent Online-Anteil) [BöRi98].

Erwartet wird eine Steigerung auf 40 Mrd. DM im Jahre 2003 laut ECO-Forum (www.eco.de) [Business Online, Heft 3, 1998, S. 10]; Diebold geht bereits für das Jahr 2000 von diesem Volumen (ca. 30-50 Mrd. DM) aus.

Für das Jahr 1998 wurde mit folgenden Umsatzzahlen kalkuliert: MyWorld 7 Millionen, Shopping24 15 Millionen, Quelle 20 Millionen [EZL-N, 19&5].

Dabei hatten die 7 Millionen Internet-Nutzer im Jahre 1998

- 25% bereits einmal Produkte online bestellt
- 31% bereits einmal Online-Dienstleistungen abgerufen.

Dabei wurden dann die folgenden Zahlungsmittel verwendet (bezogen auf alle Nutzer, von denen nur wenige online gekauft haben):

- 10,0% auf Rechnung (d.h. Überweisung oder Scheck)
- 7,9% per Kreditkarte
- 6,2% per Nachnahme
- 5,5% per Bankeinzug
- 1,1% per Vorkasse

3.1.2 Branchen

Werbung

Im Bereich der Online-Werbung wurde der Weltumsatz für 2000 auf 5,1 Milliarden USD geschätzt. Um ein derartiges Wachstum zu erreichen, ist jedoch eine bessere Fokussierung auf Kundengruppen erforderlich sowie auf Werbe-Techniken, mit denen diese besser erreicht werden können. Ansonsten ist nicht zu erwarten, daß sich die Steigerung von Investitionen in Online-Werbung rechnen wird.

In Deutschland lag der Werbe-Etat 1998 bei 40 Millionen DM, bis zum Jahr 2000 soll sich dieser auf 350 Millionen DM erhöhen. Dies ist das Ergebnis einer Forsa-Umfrage bei den 500 größten werbungstreibenden Unternehmen in Deutschland. Mit 20 Milliarden DM bestreiten sie 90% des gesamten Werbeumsatzes in Deutschland. Folglich kann davon ausgegangen werden, daß der Anteil der Online-Werbung in 2000 bei ca. 1,5 Prozent des Gesamtumsatzes liegen wird.

Online-Handel mit Computern

Dell's Online-Umsatz mit Privatkunden und Kleinunternehmen lag 1998 in Höhe von 500 Millionen USD. Cisco verkaufte Netzwerkkomponenten im Werte von 1 Milliarde USD.

Buchhandel

In Deutschland werden ca. 760.000 Bücher angeboten. Allein für ein CD-Verzeichnis dieser Bücher waren bis vor kurzem noch mehrere Tausend DM zu bezahlen. Heute steht es allen kostenlos unter www.buchhandel.de zur Verfügung. Diese Maßnahme macht nicht nur die Online-Bestellung schmackhaft, sondern lädt auch ein zum Recherchieren von Referenzen für Diplomarbeiten. Das Gesamtvolumen des Buchhandels liegt bei ca. 20 Mrd. DM, davon entfallen etwa 4,7 Mrd. DM (also ca. 25%) auf den Versandhandel. Dieser Anteil nimmt eine Spitzenposition im Versandhandel ein und erklärt, warum sich Bücher so einfach über das Web verkaufen lassen. Trotzdem liegt der Online-Anteil am Gesamtvolumen immer noch unter 1%, also ca. 200 Mio. DM.

Allgemeiner Versandhandel

Alle größeren Versandhandelsunternehmen wie Otto, Quelle, Karstadt sind heute im Internet präsent. Allerdings wird kaum verlautbart, ob der Online-Handel inzwischen rentabel ist oder weiterhin noch Anschubfinanzierungen erforderlich sind. Den folgenden Daten liegen Presseerklärungen der jeweiligen Anbieter sowie Daten ihrer jeweiligen Web-Sites zugrunde.

Ob der Internet-Handel boomt oder erst in den Startlöchern steht, ob es in erster Linie die klassischen Versandhandelsprodukte sind oder die digitalen Güter und Dienstleistungen, die im Internet gefragt und verkauft werden - darüber streiten sich noch die Geister. Anbieter lassen sich nur ungern in die Karten schauen und repräsentative Markterhebungen sind ebenfalls rar. Zu einigen größeren Anbietern von Shopping-Malls bzw. Internet-Kaufhäusern haben wir hier einige Daten zusammengetragen.

- **"Netzmarkt"** (<http://www.netzmarkt.de>) gilt als der Pionier unter den Shopping-Malls in Deutschland. Bereits im Dezember 1995 ging man ins Internet. Die Medienagentur Zeutschner in Erlangen ist der Betreiber von Netzmarkt. Netzmarkt war 1998 der einzige große "Electronic Commerce"-Anbieter im Internet, der seine Nutzungszahlen durch die IVW (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V.) überprüfen läßt. Die Zahlen vom November 1998 zeigen 429.940 Nutzungen ("Visits") und über 1,5 Mio. Page Impressions (siehe zur Terminologie auch Kapitel XXX). Das ist innerhalb von sechs Monaten in etwa eine Verdopplung. Laut "Business Online" ist Netzmarkt der meistbesuchte Internet-Shop in Deutschland. Zur wirtschaftlichen Situation sagt der Betreiber, daß man von Anfang an schwarze Zahlen geschrieben habe. Umsatzzahlen werden allerdings für den gesamten Bereich des Netzmarktes nicht genannt. Für einzelne Shops, es gibt davon momentan 20, sind solche Zahlen bekannt. Das Musikhaus Thomann hat über Netzmarkt 1997 800.000 DM umgesetzt und 3.000 neue Kunden gewonnen. Die Firma Felice (Mobilfunk) hat ebenfalls 1997 einen sechsstelligen Umsatz erwirtschaftet - bei einer Monatsmiete von 350 DM. Aus diesen Zahlen läßt sich vielleicht abschätzen, daß der gesamte Umsatz bei Netzmarkt 1998 bei einem zweistelligen Millionenbetrag liegen könnte [<http://www.netzmarkt.de/presseclub/prc1043.htm>, <http://www.netzmarkt.de/presseclub/prc1047.htm>].
- **MyWorld** (<http://www.my-world.de>) ist die Shopping-Mall des Karstadt-Konzerns, die im Oktober 1996 ins Internet ging. Monatlich besuchen etwa 300.000 Nutzer das Internet-Kaufhaus. Ob diese Zahl mit den "Visits" des Netzmarktes vergleichbar ist, erscheint eher fraglich. Karstadt meldet seine Visits jedenfalls nicht dem IVW. Zum ersten Mal äußerte sich Karstadt 1998 auf der Cebit Home zu Umsatzzahlen. Für 1998 waren sieben Millionen DM Umsatz geplant, 1997 waren es hingegen erst 700.000 DM. Gegenwärtig hat man noch nicht die Gewinnzone erreicht, mein aber, dies innerhalb der nächsten drei Jahren zu schaffen. Geplant ist die Expansion einerseits ins europäische Ausland - österreichische Kunden werden dabei als erste das Angebot von MyWorld nutzen können. Andererseits will man über Terminalsysteme, die in Tankstellen, Bahnhöfen

oder Kaufhäusern aufgestellt werden sollen, auch Kunden erreichen, die nicht über einen Internet am Arbeitsplatz oder zuhause verfügen [<http://www.karstadt.de/wir/mitteilungen/presse-980826-4.html>]

- Das Versandhaus **Quelle** (<http://www.quelle.de>) ist im Bereich der "neuen Medien" schon immer aktiv gewesen. Im BTX-System wurden 1995 immerhin 70 Millionen DM umgesetzt (Darunter fallen allerdings nicht nur Bestellungen von Endkunden, sondern auch von Agenturen und anderen Großbestellern). Auch in verschiedenen Projekten des TV-Shopping war und ist man aktiv. Im Bereich des Internet sieht man sich heute nach eigenen Angaben als Marktführer. 150.000 "Visits" (jedoch ohne Prüfung durch den IVW) gibt es gegenwärtig auf www.quelle.de monatlich. 1998 will man 20 Millionen Mark umsetzen. Diese Zahl bezieht sich ausschließlich auf klassische Endkunden und nicht auf interne Bestellungen von Filialen und auf Sammelbesteller. Der Erfolg des Internet führt nun interessanterweise zum Aus für die Quelle-CD-ROM, die im September 1998 zum letzten Mal in einer Auflage von 500.000 Stück erschien. Die Einnahmen über T-Online erreichten 1997 rund 76 Millionen Mark. 1998 erwartet man hier eine Umsatzsteigerung auf etwa 80 Millionen Mark [http://www.quelle.de/cgi/print/file=/unternehmen/presse/pm_internet.html].
- Relativ spät erst, im Oktober 1997, startete der **Otto-Versand** mit einer eigenen Mall im Internet unter dem Namen "Shopping24" (<http://www.shopping24.de>). Bereits nach sechs Monaten lag der Monatsumsatz der dann insgesamt 13 Anbieter in einem siebenstelligen Bereich. 1997 gab der Otto-Versand an, bereits 420 Millionen DM Umsatz im Online-Geschäft (außerhalb des Internet) zu tätigen (darunter auch Agenturumsätze).
[http://www.shopping24.de/mall-cgi-bin/cfilter?pWkorbId=1388537219784360&pFile=/mallbilder/html/information/index_presse.html]
- XXX Shop.de???
- XXX www.deutsche-bank.de/shop ???

3.1.3 Informationstechnologie und Medien

Fallstudie: „Cerberus“

Seit Januar 1996 verkauft Cerberus Musikstücke über das Internet. Offensichtlich waren die Umsätze nicht ausreichend, um Musik ausschließlich über das Internet zu vertreiben. Daher gründete das Unternehmen zusätzlich eine Ladenkette „High Street Retail Outlet“. Im Oktober 1998 startete Cerberus dann den „Virtual Record Store“ – ein Multimedia-Kiosk, mit dessen Hilfe Kunden aus 50.000 Musikstücken auswählen und auf ihre eigene CD aufnehmen können. Anschließend wurde mit Levi Strauss, Inc. Ein Abkommen getroffen, demzufolge in jedem europäischen Jeans-Geschäft ein Virtual Record Store installiert wird. Dieses System wird wöchentlich durch Lieferung neuer CDs, also unabhängig vom Internet, aktualisiert. Am Beispiel von Cerberos ist zu erkennen, daß das Internet noch nicht reif genug ist, um als einziger Vertriebskanal im Musikmarkt genutzt zu werden.

4 Electronic Commerce in der Volkswirtschaft

Volkswirtschaftliche Fragestellung abstrahieren von den Interessen, Entscheidungen und Randbedingungen einzelner sog. Wirtschaftssubjekte – also Privatpersonen, Unternehmen und dem Staat selbst. Das Interesse des Ökonomen gilt somit hochaggregierten Kennzahlen und den Mechanismen, die diese Zahlen beeinflussen. volkswirtschaftliche begründete Interessenschwerpunkte des Electronic Commerce sind daher

- spezifische Wirtschaftsformen, die sich aus der Nutzung des Internet ergeben,
- die Rolle des Staates als Regulierer der ökonomischen Rahmenbedingungen sowie
- der verstärkte Einfluß der internationalisierten Handels auf das lokale ökonomische Gefüge.

4.1 Rechtliche Rahmenbedingungen

Nicht ohne Grund gilt die Juristerei als Königsdisziplin der gesellschaftswissenschaftlichen Fakultäten. Sie durchdringt fast jede soziale Interaktion, die sich außerhalb der Privatsphäre ereignet und versucht, in jahrhundertelanger Tradition diese Interaktion in Form stark abstrahierender Analyse- und Designwerkzeuge zu beschreiben und zu normieren. Wenn wir uns also mit Fragestellungen des Electronic Commerce beschäftigen wollen, ist es folglich sinnvoll, das Rahmenwerk, welches den elementaren Handelsprozessen der traditionellen Ökonomie zugrundeliegt, zu beleuchten. Dabei können nur die besonders relevanten Bereiche des Vertragsrechts, des Datenschutzes sowie einiger anderer Schwerpunkte behandelt werden. Diese Bereiche korrespondieren jeweils mit technischen Lösungen, die weiter hinten im Buch illustriert werden.³

4.1.1 Vertragsrecht und Internet

Im virtuellen Raum des Internet Verträge zu schließen, berührt zivilrechtliche Fragen des Vertragsrechts sowie spezifische rechtliche Regulierungen des Electronic Commerce. Traditionell kommt ein Vertrag zustande durch den Austausch von Willenserklärungen. Diese lassen sich als „atomare Bausteine des Rechtsverkehrs“ auffassen, aus denen durch Kombination komplexere Konstrukte wie beispielsweise ein Vertrag komponiert werden können. Eine Willenserklärung ist ein freier Entschluß einer natürlichen Person zur Durchführung einer Handlung. Eine solche Handlung könnte beispielsweise eine Leistung sein, z.B. einen Geldbetrag zu zahlen oder Ware zu liefern. Nach dem BGB ist ein Vertrag gerade die Vereinbarung gegenseitiger Leistungen. Beim Kaufvertrag wird beispielsweise „Geld zahlen“ gegen „Buch liefern“ getauscht. Dieser Tausch ist idealerweise transaktional im technischen wie im juristischen Sinne. Technisch ist dies jedoch nicht immer möglich: Liefert ein Online-Shop eine Software an den Käufer aus und zahlt dieser nicht, besteht keine Möglichkeit zum „Rollback“. Nur über den juristischen Umweg des Gesetzes kann dann das „Rollback“ erzwungen werden. Der Jurist unterscheidet hier verschiedene Möglichkeiten, die Transaktion zu einem definierten Ausgang zu führen: entweder wird die Zahlungsleistung erzwungen oder durch eine andere Leistung ersetzt. Das BGB stellt für solche Zwecke ein generisches Regelwerk dar, das für konkrete Rechtsgeschäfte konkretisiert und angewendet werden kann. Grundsätzlich lassen sich mit Hilfe dieses Regelwerks und den Grundbausteinen wie etwa Willenserklärungen komplexe Vertragsstrukturen konstruieren:

Man stelle sich vor, Detlef aus Deutschland, Gustaf aus Großbritannien und Berthold aus Brasilien vereinbaren einen Ringtausch: Detlef liefert Autos an Berthold, Berthold Kaffee an Gustaf und dieser Tee an Detlef. Um die Sache zu verkomplizieren, hat Detlef Stefan als Stellvertreter bevollmächtigt. Durch die Vollmachterteilung (wieder eine Willenserklärung) kann Stefan im Namen von Detlef agieren (d.h., Willenserklärungen aussprechen). Insgesamt sind folglich drei Leistungen vereinbart, die einen multilateralen Vertrag ergeben, der vom Kaufvertrag im Sinne des BGB etwas abweicht (es fließt kein Geld, es sind mehr als zwei Parteien). Da dieses Volumen in der Größenordnung einiger Millionen Euro liegt, erfordert Bertholds Gesetzgeber die Schriftform, während bei Detlef eine mündliche Willenserklärung ausreicht. Das Transaktionsproblem liegt hier zum einen im Zustandekommen des Vertrags (Erfordernis der Schriftform, Vereinbarung des Gerichtsstands etc.), zum anderen

³ Insbesondere die Verfahren zur Unterstützung von Datenschutzmaßnahmen und zum elektronischen Vertragsschluß.

wieder in der Sicherung eines Zugangs aller Leistungen in ihrer vollständigen Quantität und Qualität.

Wie das Transaktionsproblem zeigt, liegt eine wesentliche Voraussetzung in der Festlegung eines einheitlichen Vertragsrechts. Dieses wird zum einen bestimmt durch das internationale Vertragsrecht und zum anderen durch Regulierungsvorschriften, die auf die besonderen Umstände des Electronic Commerce abzielen. Dabei ist zunächst kein Unterschied zwischen dem elektronischen Vertragsschluß und dem herkömmlichen (auf Papier) gegebenen, wenn Willenserklärungen auf elektronischem Wege ausgetauscht werden können, wenn die Authentizität der Person gesichert ist (siehe hierzu Kapitel XXX). Damit (und auch durch andere Merkmale) entstehen allerdings zusätzliche, Electronic-Commerce-bedingte Anforderungen, die eine juristische Sonderbehandlung erfordern:

- Sicherstellung der Rechtswirksamkeit elektronisch übermittelter Willenserklärungen
- Sicherung geistiger Rechte
- Maßnahmen für den Verbraucherschutz
- Maßnahmen zum Datenschutz
- Steuerrechtliche Fragen

Da sich ein Vertrag in eine Anzahl Willenserklärungen zerlegen läßt, ist zu verifizieren, daß diese Erklärungen auch tatsächlich von den Personen abgegeben wurden, die als Vertragsparteien beteiligt sind. Zudem ist sicherzustellen, daß die Integrität des Vertrages gewahrt bleibt, d.h., daß weder während des Unterzeichnungsprozesses noch dem Zustandekommen des Vertrages Modifikationen unerkannt vorgenommen werden können.

Kompliziert wird es, wenn ein Vertrag implizit, d.h. ohne den Austausch schriftlicher oder sonstwie verarbeitbarer Willenserklärungen zustandekommt. Dies ist heute eher der Regelfall: Beim Online-Kauf liegt weder beiden Seiten ein einheitliches Dokument vor, das als gemeinsam unterzeichneter Vertrag den Leistungsaustausch regelt, noch existieren über das WWW standardisierte Prozeduren für einen fairen Austausch von Willenserklärungen, so daß keine Partei die andere betrügen kann.

Wir können heute dennoch ökonomisch einigermaßen sicher im Internet agieren, da es heute immer noch eine Verlängerung traditioneller Wirtschaftsbeziehungen in die Netzinfrastruktur hinein projiziert. Und in der traditionellen Ökonomie haben sich über Jahrhunderte soziale Gefüge und Protokolle herausgebildet, die einen Regelverstoß auf die eine oder andere Weise sanktionieren. In der Internet-Ökonomie können allerdings ganz andere Mechanismen greifen, die möglicherweise auch entsprechende Rahmenbedingungen erfordern. Im Hinblick auf den elektronischen Vertragsschluß ergeben sich hier interessante Perspektiven, die in Kapitel XXX ausführlicher beschrieben werden.

4.1.2 Das Signatur-Gesetz

Das Deutsche Signaturgesetz [SigG XXX] ist unter verschiedenen Gesichtspunkten zu betrachten: zunächst schafft es eine juristische Grundlage für die Verwendung elektronischer Signaturen. Dabei besagt es zunächst nur, daß elektronische Signaturen als rechtsverbindliche Unterschrift anerkannt werden. Hierbei sind jedoch zwei Voraussetzungen zu erfüllen: Erstens muß die zum Signieren geforderte Technologie eingesetzt werden, und zweitens muß von den beteiligten Parteien die elektronische Signatur der manuellen Unterschrift gleichgestellt werden. Die erste Bedingung regelt die Signaturverordnung [SigV XXX], in der festgelegt wird, welche technischen und organisatorischen Maßnahmen zu ergreifen sind, um eine Signatur im Sinne des Gesetzgebers leisten zu können. Die zweite Bedingung wird erfüllt, wenn sich z.B. deutsche Behörden dazu entschließen, neben der manuellen Unterschrift auch die elektronische Signatur anzuerkennen. Dies kann sich auf Bauanträge, Steuererklärungen etc. beziehen. Zu diesem Zweck werden zur Zeit fast viertausend Vorschriften durchforstet, um sie der neuen Gesetzgebung anzupassen.

Der Wirtschaft sowie Privatpersonen ist es freigestellt, die elektronische Signatur anzuerkennen und zu verwenden. Das Gesetz schreibt noch nicht einmal vor, Signaturen nach seinem geforderten Standard verwenden zu müssen; es legt lediglich Mindestanforderungen fest, nach deren Einhaltung eine Signatur vor Gericht als rechtsverbindlich anerkannt wird. Dies entlastet die Beweisführung bei Rechtsstreitigkeiten ganz erheblich.

Eine wichtige weitere Intention des Signaturgesetzes ist es vor allem auch, Technologieführerschaft zu forcieren. Dabei ist zu berücksichtigen, daß Deutschland im Bereich der SmartCard-Entwicklung weltweit führend ist.⁴ Um diesen Vorsprung zu fördern, kann die Erfordernis Token-basierter Signatursysteme (d.h. der Einsatz von Smart-

⁴ Siemens hält beispielsweise den Löwenanteil bei der Produktion von SmartCard-Chips.

Cards) die Verbreitung dieser Technologie weiter fördern. Außerdem hilft eine Norm auf international als sehr hoch empfundenem Niveau, Standortvorteile zu schaffen, da ausländische – möglicherweise weniger restriktive – Vorschriften nicht akzeptiert werden würden. Wenn also beispielsweise aufgrund der EU-Richtlinie Kom(1998)297 in einem anderen europäischen Land Signaturen mit Hilfe eines Schlüssels, der auf der Festplatte gelagert wird, vorgenommen werden dürfen, so werden diese in Deutschland nicht anerkannt. Auch die Gleichstellung der elektronischen Signatur wird von der EU vorgesehen. Hier wird es ebenfalls zu Harmonisierungsproblemen kommen, wenn die Umsetzung der Richtlinie auf unterschiedlichem Niveau erfolgt.

Unter den ersten Herausgebern elektronischer Zertifikate befindet sich die Telekom mit ihrem Tochterunternehmen TeleCash, vormals einem Gemeinschaftsunternehmen mit der IBM Deutschland. Über ihre T-Points steht eine Infrastruktur zur Registrierung des eigenen öffentlichen Schlüssels zur Verfügung. Dabei erhält der Kunde eine SmartCard mit dem entsprechenden privaten Schlüssel. TeleCash betreibt einen Zertifizierungsdienst, über den von anderen Teilnehmern das Zertifikat für den öffentlichen Schlüssel abgerufen werden kann. Dieser Service kostet pro Jahr über 100 DM. Langfristig ist zu erwarten, daß die Gebühren für die Erstaussstellung bei ca. 30 DM sowie die jährlichen Gebühren bei ca. 10 DM liegen werden. Folglich kann nicht davon ausgegangen werden, daß breite Bevölkerungsschichten über zertifizierte Signaturschlüssel verfügen werden.

4.1.3 Die Rolle der Europäischen Kommission

Beim Stichwort „Regulierung“ denken wir zunächst an den nationalen Gesetzgeber, obwohl sich doch Electronic Commerce ohne Rücksicht auf nationalstaatliche Grenzen vollzieht. Da das andere Extrem einer globalen Steuerung mittelfristig undenkbar ist, stellt das Gebiet der Europäischen Union einen noch ausreichend begrenzten, gleichzeitig jedoch einflußreichen Wirtschaftsraum dar. Unabhängig von der Frage, ob und welche Rahmenbedingungen für den Electronic Commerce zu schaffen sind, ist über Verfahren zur Festlegung von EU-Richtlinien ein Instrument geschaffen worden, das es erlaubt, zentral ausgearbeitete Vorgaben der EU innerhalb einer Frist von drei Jahren in die jeweilige Gesetzgebung der Partnerstaaten umzusetzen. Diese Richtlinien betreffen Aspekte des Datenschutzes, der Verwendung elektronischer Signaturen, des Schließens von Verträgen über das Internet, des Verbraucherschutzes etc. Häufig sind diese Richtlinien innerhalb der EU umstritten, da unterschiedliche nationale Interessen der Partnerländer sich nicht immer vollständig harmonisieren lassen. Dies kann dann zu sehr abstrakten Vorschriften und Mindestanforderungen führen, die großen Spielraum für inkompatible Umsetzungen lassen. Der Erfolg kann dann nur noch in der Einhaltung eines Mindeststandards gemessen werden, jedoch nicht in einer garantierten Harmonisierung.

EU-Richtlinien werden von der EU-Kommission ausgearbeitet und anschließend vom Parlament und dem Rat verabschiedet. Danach besteht für die Mitgliedsstaaten eine dreijährige Frist zur Umsetzung der Richtlinie in lokales Gesetz. Wird diese Frist nicht eingehalten, droht ein Bußgeld. In den letzten Jahren sind eine Reihe von Richtlinien zu Themen wie zum Beispiel zum Daten- und Verbraucherschutz erlassen worden. Aktuell werden Entwürfe zur Verwendung elektronischer Signaturen, zum Electronic Commerce im allgemeinen sowie zur Verwendung elektronischen Geldes ausgearbeitet:

- EU-Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 über den **Schutz personenbezogener Daten**. Diese Richtlinie wurde bis zum April 1999 nur von Schweden, Großbritannien, Griechenland und Italien umgesetzt. In dieser Richtlinie werden die Rechte der Bürger im Hinblick auf personenbezogene Daten präzisiert. Insbesondere sieht die Richtlinie eine zentrale unabhängige Kontrollbehörde vor, der seitens der Unternehmen ein Datenschutzbeauftragter zu melden ist. Um dieses Verfahren etwas zu entbürokratisieren, kann ein Unternehmen auch freiwillig einen betrieblichen Datenschutzbeauftragten ernennen. Dieser hat Daten, die besonders schutzwürdig sind, besonders zu behandeln (rassische und ethnische Herkunft, politische, religiöse oder philosophische Überzeugungen oder auch Daten über Gesundheit und Sexualleben). Insbesondere dürfen Entscheidungen, die auf diesen Daten beruhen, nicht automatisch herbeigeführt werden. Dies steht im klaren Widerspruch zu den Möglichkeiten und der geschäftlichen Praxis in den USA, wo Kundenprofile als handelbares Gut betrachtet werden. Aus diesem Grund birgt die Richtlinie besonderes Konfliktpotential, da sie die Weitergabe der Daten nur an Unternehmen zuläßt, die sich in einem Land befinden, das ebenfalls das Datenschutzniveau der EU vorschreibt. Dies gilt sicherlich nicht für die USA. Hier ist noch offen, inwieweit multinationale Unternehmen Daten auch in Drittländer transferieren können, in denen sie ihre zentrale Datenverarbeitung betreiben.
- EU-Richtlinie 97/7/EC zum **Verbraucherschutz** im Hinblick auf „Fernverträge“ (XXX), 97/17/EC. Diese Richtlinie regelt Bedingungen und Rechte, unter denen Verbraucher über das Internet Waren bei Online-Shops erwerben können. Beispiele für diese Bedingung sind:
 - Der Anbieter muß seine Identität und Adresse bekanntgeben,

- wesentliche Eigenschaften der Online angebotenen Güter sind zu beschreiben,
- Preis und Lieferkosten sind inklusive aller Steuern zu nennen,
- Zahlungs- und Lieferbedingungen sind zu nennen,
- es ist auf das Rücktrittsrecht innerhalb einer Woche hinzuweisen,
- die Periode, innerhalb derer das betreffende Angebot gilt etc.

Ferner erfordert diese Richtlinie eine *schriftliche Bestätigung* der Online-Bestellung. Es ist noch zu klären, inwieweit hierbei Ersatz durch die Verwendung einer elektronischen Signatur geschaffen werden kann.

- Richtlinie zur Verwendung **elektronischer Signaturen**. Hierbei sind etliche Rahmenbedingungen zu vereinheitlichen, bevor zwei Vertragsparteien aus unterschiedlichen Mitgliedsstaaten ihre elektronischen Signaturen gegenseitig als rechtswirksam anerkennen können. Beispielsweise ist festzulegen, wann eine Willenserklärung der Schriftform bedarf – und nur der Schriftform, nicht jedoch einer notariellen Beglaubigung. Die technischen Anforderungen des Erwerbs und der Verwendung elektronischer Signaturen sind zu vereinheitlichen. Auch wenn bereits heute ein einheitliches technisches Verfahren eingesetzt wird, besteht das eigentliche Problem erst in der organisatorischen Umsetzung. Während in Deutschland auf ein hohes technisches Niveau zur Gewährleistung von Authentizität gesetzt wird, zielt die EU-Richtlinie auf eine teilweise Selbstregulierung dadurch ab, daß Zertifizierungsstellen für die Authentizität ihrer Kunden haften. Dabei liegt bei einem Streitfall die Beweislast auf der Seite CAs bzw. ihrer Kunden, daß die verwendete Signatur tatsächlich korrekt war. Nach dem deutschen Signaturgesetz verhält es sich umgekehrt: juristisch formuliert, geht man von einer sog. Beweisvermutung (XXX?) aus. Hierbei ist nicht bei jedem Einzelfall zu prüfen, ob tatsächlich eine Willenserklärung anhand eines korrekten Zertifikats vorlag. Knapp formuliert ist die Signatur in Deutschland teuer bei der Benutzung, reduziert aber den Aufwand der Beweisführung. Nach europäischer Vorstellung ist Erwerb und Verwendung billig, jedoch die Beweisführung teuer.

Im folgenden sind einige weitere Punkte genannt, bez. derer die EU-Richtlinie von dem deutschen Signaturgesetz abweicht:

- Das deutsche Signaturgesetz legt sich technologisch auf das Public-Key-Verfahren fest, während die EU-Richtlinie ausdrücklich offenläßt, ob ein symmetrisches oder asymmetrisches Verfahren eingesetzt wird.
- Ferner unterscheidet die EU-Richtlinie zwischen der „elektronischen Signatur“ im allgemeinen und der „qualifizierten digitalen Signatur“ im speziellen. Nur letztere entspricht dem deutschen Signaturgesetz.
- Das deutsche Signaturgesetz sieht eine staatliche Lizenzierung und Beaufsichtigung von Zertifizierungsstellen vor, während die EU-Richtlinie liberaler ist: Hier werden freiwillige Akkreditierungssysteme bevorzugt, bei denen sich Zertifizierungsstellen freiwillig einer Aufsicht unterziehen *können*.
- Haftung. Das deutsche Gesetz sieht keine Haftungsregelungen für die Herausgeber von Zertifikaten vor, während der europäische Entwurf dies ausdrücklich vorsieht.
- Richtlinienentwurf eines **Rechtsrahmens für den elektronischen Geschäftsverkehr in Europa**. Diese Richtlinie befaßt sich mit allen juristischen Aspekten, die Dienstleistungen der Informationsgesellschaft betreffen. Sie erstreckt sich auf alle Beteiligten (Unternehmen und Privatpersonen auf Anbieter- und Nachfragerseite) sowie auch werbe- oder sponsorenfinanzierten Services. Sie betrifft somit z.B. auch online-Zeitungen, -Datenbanken und -Banken; online-Anwälte, -Steuerberater und -Immobilienmakler oder auch Video-on-Demand-Anbieter. Festgelegt werden Regelungen zur Standortwahl eines Unternehmens und Gerichtsstandsvereinbarungen. Auch im Zeitalter frei reisender „e-Lancer“ kann damit ermittelt werden, welchen Sitz beispielsweise ein Unternehmer hat, dessen Web-Server auf Mauritius betrieben wird, dessen Arbeitsplatz eine 1-Zimmerwohnung in Paris ist, dessen e-Mail-Adresse auf „.de“ endet und dessen Haupttätigkeitsbereich Großbritannien ist.⁵ Zielsetzung dieser EU-Richtlinie ist zudem, den elektronischen Geschäftsverkehr dadurch zu fördern, daß Formvorschriften zugunsten elektronischer Dokumente verändert werden. In einigen Staaten ist beispielsweise die Schriftform von einem bestimmten Volumen an vorgeschrieben. Damit kann diese Richtlinie als Ergänzung zu vorhergehenden (insb. zur elektronischen Signatur) verstanden werden. Eine effizient durchführbare Schadensersatzregelung sowie grenzüberschreitende Sanktionierungsmöglichkeiten von Regelbrechern sind genauso Gegensatz der Direktive wie eine einheitliche Position zu Themen wie z.B. „Spamming“. Insbesondere bei dieser Fragestellung nehmen Vertreter der Werbebranche und des Direktmarketingbereichs zur Zeit (1. Quartal 1999) erheblichen Einfluß auf diese Gesetzgebung.

⁵ Zur Klärung des Rätsels: Es gilt hier die Hauptniederlassung, d.h., der Ort, an dem das Gewerbe angemeldet wurde (z.B. Hamburg).

- **Richtlinienentwurf für die Zulassung von E-Geld-Instituten** (KOM(98)0461). Hierbei wird der grundsätzliche Charakter elektronischen Geldes definiert sowie Bedingungen festgelegt, zu denen Geldinstitute elektronisches Geld emittieren dürfen. Dieser Richtlinienentwurf befindet sich nach in der Diskussion (April 1999) und dürfte erst im zweiten Halbjahr 1999 verabschiedet werden.

4.2 Neue ökonomische Modelle

Warum werden im Zusammenhang mit Electronic Commerce eigentlich so viele „neue Geschäftsmodelle“ diskutiert? Worin besteht der Unterschied zum bisherigen Ansatz, was hat sich verändert? Im wesentlichen kann man sagen, daß die Gewinnung und Verarbeitung von Information billiger geworden ist. Dies gilt sowohl für den außerbetrieblichen als auch für den innerbetrieblichen Bereich. Unterschiedlichste Technologien helfen heute nicht nur, ein Vielfaches an Daten zu speichern, sondern ihnen auch zusätzliche Information abzurufen. Heute helfen Datawarehousing-Anwendungen, auch kleine Informationshäppchen aus einem Nebel von Daten zu fischen. Mit Hilfe von Data-Mining-Anwendungen wird sogar versucht, diesen Prozeß zu automatisieren.

Neben dem verfeinerten Instrumentarium zur Informationsgewinnung liegen weitere Einflußfaktoren in der Standardisierung und Vernetzung von Unternehmen. Nur wenn Amazon.Com Millionen von Kunden bedient und Zigtausende von Büchern im Vorrat hält, wird es profitabel, Profilinformation zu verarbeiten und daraus Kaufvorschläge für den nächsten Kunden abzuleiten. Das Verhältnis von Investitions- zu Betriebskosten verändert sich extrem stark in Richtung von Grenzkosten, die gegen Null laufen: Ein News-Forum einzurichten kostet gewissen Aufwand, sein Betrieb kann jedoch automatisch erfolgen. Wenn nun auch noch die Telekommunikationskosten gegen Null tendieren und gleichzeitig das Potential besteht, weltweit ein Millionenheer von Nutzern zu bedienen, so „rechnet“ sich der Betrieb des Systems sogar bei minimalem Deckungsbeitrag je verkaufter Einheit.

Schließlich hilft die Standardisierung im Bereich der Kommunikation (TCP/IP, HTTP), der Darstellung (HTML, XML/XSL) geschäftlicher Anwendungen (EDI, SAP) sowie bei der zukünftigen Sicherheits- und Vertrauensinfrastruktur, kostspielige Hindernisse im Geschäftsverkehr aus dem Weg zu räumen. Ansonsten behindern Konvertieraktivitäten oder unüberwindbare Inkompatibilitäten mögliche Geschäftsverbindungen von Beginn an.

Als extreme Extrapolation kann man sich die Welt von morgen damit so vorstellen: zum Nulltarif steht beliebig lang und bei (fast) beliebiger Bandbreite jede bereitgestellte Information weltweit in einheitlicher und verarbeitbarer Form zur Verfügung. Die Speicherung und Verarbeitung dieser Information erfolgt quasi kostenlos. Damit kann eine Optimierung von Geschäftsprozessen – sobald sie erkannt wurde – durchgeführt werden. Allein die Investition in den veränderten Prozeß (Softwareentwicklungs und -Installationsaufwand) spielt für diese Entscheidung eine Rolle. Diese Prozeßveränderung ist, unabhängig von der Anzahl betroffener Transaktionen, mit fixen Kosten verbunden.

Zusammengenommen helfen diese „neuen Parameter“, die Umlaufgeschwindigkeit und die Granularität der Information zu verbessern. Die Wahrnehmung der Welt durch das Medium der Informationstechnologie ist damit sehr viel feinkörniger geworden. In einer solchen Welt „rechnen“ sich damit Maßnahmen, die traditionell als absurd oder zumindest unrentabel abgetan werden würden:

- Regalfläche im Supermarkt erlangt unmittelbaren Wert und kann meterweise den Herstellern von Lebensmitteln vermietet werden. Traditionell wäre die softwaretechnische Verwaltung dieser Daten bereits zu kostspielig gewesen. Auch die Berücksichtigung von Preisdifferenzen, die für diese Mietfläche vielleicht nur im Pfenigbereich liegen, war zuvor durch zu hohe Verarbeitungskosten der IT-Infrastruktur sinnlos.
- Seit einiger Zeit setzt der Metro-Konzern in seinen Zentren LCD-Displays zur Kennzeichnung der Artikelpreise ein. Diese Technik ermöglicht es theoretisch, Preise nachfragegesteuert anzupassen: Wenn sich zu Spitzenzeiten Käufer an den Kassen drängen und entsprechend viel Personal erforderlich ist, könnte durch einen Zuschlag diese Spitzenlast auf Uhrzeiten verdrängt werden, zu denen die meisten Kassen leer stehen.
- Bei nahezu kostenloser Rechenleistung lohnt es sich, Rationalisierungsgewinne aus der Optimierung der Vertriebslogistik zu generieren: Wenn ein Pharmakonzern Informationen hätte, anhand derer der exakte Arzneimittelbedarf tages- und apothekengenau ermittelt werden kann, könnten Kunden bei Spitzenlast-Situationen (d.h. bei Grippewellen) besser bedient werden. Genau zu diesem Zweck werden in den USA Systeme installiert, mit deren Hilfe Bedarfe für den nächsten Tag vorausgesagt werden können, indem übliche Verbreitungswege und -geschwindigkeiten von Grippewellen eingesetzt werden, um Lager und Apotheken mit den richtigen Mengen versorgen zu können.

- Marktinformation wird aus Kundenprofilen abgeleitet. Diese Daten liegen damit von Beginn an in strukturierter und damit leicht verarbeitbarer Form vor. Somit lassen sich nicht nur „grobkörnige“ Informationen wie z.B. Firmenadressen veräußern, sondern auch stark verfeinerte Daten wie z.B. Verhaltensmuster bei Flugbuchungen, nachgefragte Produktkonstellationen, oder auch Interessenprofile auf der Basis von „AdClicks“ – also den angeklickten Werbebannern.
- Schließlich ist es für Online-User denkbar, daß sie sich mit Hilfe moderner Datenschutztechnologien, wie z.B. P3P (siehe dazu auch Kapitel XXX), die Weiterverarbeitung persönlicher Daten vom Online-Anbieter in Form von Rabatten auszahlen lassen. Auch hierbei handelt es sich möglicherweise um Pfennigbeträge, die jedoch erst durch die preiswerte IT-Infrastruktur effizient verarbeitbar werden.

Aus diesen Beispielen ist zu entnehmen, daß aus den unterschiedlichen Rationalisierungsgeschwindigkeiten im logischen und im physikalischen Bereich Optimierungsmöglichkeiten entstehen. Noch drastischer wirken sich jedoch die neuen Parameter in einer reinen Ökonomie der digitalen Güter („Soft-Goods“) aus: Für ein solches Gut ist ein einmaliger Herstellungsaufwand zu kalkulieren, während der Vertrieb fast zum Nulltarif erfolgen kann. Insbesondere bei Soft-Goods können Standardisierung, Vernetzung und Preisverfall ebenfalls zur Erstellung, Kombination und Distribution dieser Güter genutzt werden:

- Ein Musiker kann seine Werke direkt im Internet anbieten. Diese Kosten belaufen sich dabei auf die Einrichtung einer Homepage. Weitere Betriebskosten lassen sich in der NetEconomy ignorieren. Bietet der Musiker das Stück zu dem Preis an, den er als Honorar vom Verlag erhalten würde und setzen wir voraus, daß der Absatz in ähnlichen Stückzahlen erfolgt wie in der traditionellen Ökonomie, sollte ein einzelnes Musikstück für weniger als 0,20 Euro zu erwerben sein. Nun kann jedoch angenommen werden, daß das Kaufverhalten bei diesen Preisen durchaus anders ist als bei CD-Preisen jenseits von 10 Euro. Spekulative Käufe werden zunehmen. Andererseits ist der Verdrängungswettbewerb um die Aufmerksamkeit der Käufer weitaus härter. Mit MP3 wurde ein Audio-Kompressionsverfahren entwickelt, das es Besitzern einer ISDN-Verbindung ermöglicht, für einige Pfennige Verbindungsgebühren ein Musikstück online zu laden. Seit einiger Zeit entstanden daher Grau- und Schwarzmärkte im Internet. Für die Musikbranche droht diese Entwicklung zu einer Neudefinition der gesamten Wertschöpfungskette zu führen: CD-Produktion und Vertrieb werden überflüssig, Musikverlage als Verwalter der Verwertungsrechte am Werk werden immense Schwierigkeiten bekommen, den Absatz und Konsum dieser Produkte zu kontrollieren, und auch für Verwertungsgesellschaften wie die GEMA nehmen die Schwierigkeiten bei der Kontrolle von Verkauf und Aufführung zu.
- Bücher Online anzubieten ist seit Amazon.Com ein alter Hut. Bücher als digitale Güter stellen jedoch auch heute noch eine Herausforderung dar: Wenn der Lesekomfort eines traditionellen Buches erreicht werden kann (durch dedizierte Lesegeräte wie etwa das eBook [XXX] oder XXX) und alle haptischen Eigenschaften und Möglichkeiten nachempfunden werden können (Eselohren, Anmerkungen), sollten auch elektronische Bücher den Weg aller Soft-Goods gehen: einmal geschrieben, lassen sie sich als elektronische Dokumente für einen Bruchteil des Ladenpreises online anbieten. Evtl. können Leser sich ihr Exemplar direkt beim Printshop „um die Ecke“ ausdrucken und binden lassen, so daß der Text am Ende als Buch wieder in der Hand liegen kann. Auch dieser Prozeß dürfte die üblichen Kopierkosten von 5-8 Euro nicht überschreiten, so daß ein gebundenes Fachbuch zu einem Preis von 10-15 Euro am Ende jeden (noch) Beteiligten befriedigen kann.
- Das Internet-Softwareunternehmen Ponton Hamburg hat für den Anbieter von Schrifttypen, Linotype Library (www.fonts.de XXX?), einen Online-Shop entwickelt, mit dem Typen im Format TTF (True Type Font) und Adobe PostScript online ausgewählt, bestellt und geliefert werden können. Fonts sind damit ebenfalls aus einer Grundgesamtheit von 30.000 Exemplaren direkt durch den Endkunden auswählbar. Da dem Online-Kunden ein Applet zur Spezifikation von Font-Eigenschaften und zur Vorabansicht von Beispielen zur Verfügung steht, kann für den Anbieter der bisher sehr kostspielige Aufwand zur Produktion von Prospektmaterial und Samples entfallen. Auch hierbei reduziert sich der Aufwand für einen neuen Font auf seine Eintragung in die Datenbank des Online-Shops.
- Neben den vorgenannten Massenmärkten, von denen bereits sehr viel in der Presse berichtet wird, entstehen weitere Soft-Good-Märkte im Bereich der „Knowledge-Worker“: Diese sind beispielsweise Übersetzungsdienste, Call-Center, CAD-Designer, Gestalter von Banner-Bitmaps, Entwickler von Softwarekomponenten etc. Auch die hier gehandelten Produkte sind nicht-physischer Natur, jedoch werden sie nicht „vom Regal“ abverkauft. Vielmehr ist ihre Produktion stärker in einen Geschäftsprozeß eingebunden, wir sprechen daher auch von „Soft Services“, die vollständig über das Internet abgewickelt werden können. Soft-Services finden sich häufig im Kontext des B2B-Commerce (siehe auch Kapitel XXX zum Thema „virtuelle Unternehmen“).

Auch wenn festgestellt werden kann, daß Electronic Commerce die Korngröße ökonomisch handelbarer Einheiten drastisch verringert, rüttelt dies nicht grundsätzlich an der Basis marktwirtschaftlicher Prozesse. Immer noch optimiert jeder Marktteilnehmer an seinem Produktions- oder Dienstleistungsapparat, um am Ende den Gewinn zu maximieren. Es sind durch Standardisierung und Preisverfall lediglich die Auflösung seiner Meßinstrumente

sowie seine Steuerungsmöglichkeiten verbessert worden.

Diese Betrachtungen erfolgen aus der Perspektive des einzelnen Marktteilnehmers – sie sind also aus einer betriebswirtschaftlichen Sicht motiviert. Anders verhält es sich bei der Betrachtung aggregierter Mengen, Entscheidungen und Prozesse, die aus der ganzheitlichen Perspektive der Volkswirtschaft beobachtet werden können:

4.2.1 Klassische und neue volkswirtschaftliche Modelle

An dieser Stelle sollen keine volkswirtschaftstheoretischen Grundlagen wiederholt werden, die bereits durch Fachbücher wie XXX abgedeckt wurden. Vielmehr wollen wir uns direkt dem Electronic Commerce zuwenden und aktuelle Entwicklungen über die heutige Experimentier- und Adaptionsphase hinaus extrapolieren. Letztere ist durch hohe Kosten und teilweise unrentable Produkt- oder Prozeßentscheidungen geprägt, da der technisch-organisatorische Lernprozeß bez. neuer Geschäftsmodelle erst langsam in Gang kommen konnte. Niemandem ist heute beispielsweise klar, wieviele Wettbewerber der nationale Telekommunikationsmarkt verträgt, wieviele Anbieter von Software für Online-Shops sich langfristig halten können (viele generieren als börsennotierte Investmentmodelle heute immer noch Verluste) etc. Folglich wollen wir uns im folgenden einige Phänomene und Randerscheinungen des Electronic Commerce ansehen und sie im Anschluß – sozusagen durch „Reverse Engineering“ – mit den zugrundeliegenden Modellen in Verbindung bringen.

Wirkungen des Electronic Commerce

- **EC egalisiert.** Unabhängig von der Region besteht für alle Marktteilnehmer ein gleichartiger Zugang zur Netzökonomie. Evtl. kann sich dies sogar auf Kostenstrukturen der realen Welt auswirken, indem sich z.B. Lebenshaltungskosten auf dem Lande und in der Stadt angleichen. EC egalisiert aber auch international: Deutsche Unternehmen arbeiten mit portugiesischen, polnischen und indischen Softwareunternehmen zusammen. Je besser und preiswerter das Internet die internationale Telekooperation unterstützt, desto niedriger sind die Kommunikationsbarrieren, die heute eine gemeinsame Produktion verhindern. Schließlich egalisiert EC zwischen Unternehmen und Einzelpersonen – also letztlich der Organisationsgröße. Während ein permanenter Zugang zum Internet oder sogar der Betrieb eines Online-Shops sich zuvor nur für Unternehmen rechnete, die durch ein hohes Transaktionsvolumen die Investitions- und Betriebskosten decken konnten, ist dies heute fast zum Nulltarif und damit für jede Privatperson möglich. Wir kehren dabei zurück zum Begriff der „Volkswirtschaft“, bei dem der einzelne Bewohner als gleichberechtigtes Wirtschaftssubjekt auftreten kann – als Anbieter oder Nachfrager. Der elektronische Marktplatz entspricht somit einer „Agora“ der griechischen Antike, d.h. dem öffentlichen Raum des Marktplatzes, der von seinen Teilnehmern kostenlos betreten werden kann, der nicht nach ihrer Zugehörigkeit oder Herkunft unterscheidet und der als Pflaster eine einheitliche Infrastruktur bietet.
- **EC führt zur Hollywood-Ökonomie.** Eine Filmproduktion erweist sich immer dann als Erfolg oder Mißerfolg, wenn der Produzent keinen Einfluß mehr auf das Produkt nehmen kann. Es besteht weder die Möglichkeit, eine verbesserte Version 1.1 nachzuliefern, noch die zur Rückrufaktion und Reparatur. Sehr ähnlich verhält es sich heute mit der Produktion von Computerspielen oder CD-Roms im Edutainment-Bereich. Ein wenig kann der Erfolg des Produkts durch Marketing- und Werbemaßnahmen beeinflusst werden, aber am Weltmarkt wird es nur bestehen, wenn es durch seine inhärenten Merkmale besticht. Gleiches gilt zunehmend für die Softwareproduktion: Ein neuer Web-Browser, ein HTML-Editor, eine betriebswirtschaftlich spezialisierte Softwarekomponente muß technisch und preislich überzeugen, damit sie gekauft wird, ansonsten wird mit der Maus abgestimmt und bei der Konkurrenz gekauft. Diese Extrapolation ist natürlich überspitzt, zeigt jedoch einen Trend auf, der sich aus der Standardisierung und Globalisierung ergibt. Für den einzelnen Anbieter bedeutet Hollywood-Ökonomie damit, daß er 3-4 Flops durch einen Kassenschlager finanzieren muß, für den Käufer die Freiheit der Wahl. Hollywood-Ökonomie zeigt sich aber auch in anderen Branchen: Wagniskapital wird beispielsweise ebenfalls nach dem Schema „drei Flops, ein Erfolg“ investiert.
- **Die Evolution frißt ihre Kinder.** Menschheitshistorisch haben sich Entwicklungen wie das Rad, Schwarzpulver, Dampfmaschine oder auch gesellschaftliche Konzeptionen wie „Demokratie“ und „Staat“ in Perioden entwickelt, die sich über ein Vielfaches einzelner Generationen erstreckten. Der einzelne Mensch wurde damit in einen statischen Zusammenhang aus Bildung, Arbeit und Gesellschaft geboren und starb meistens, ohne drastische Veränderungen seiner gesellschaftlichen Umwelt erlebt zu haben. Umgekehrt konnte eine neue Generation „müheles“ eine Entwicklung repräsentieren und realisieren. Auch ohne Internet begann jedoch die Halbwertszeit des Wissens seit einigen Jahrzehnten auf Bruchteile der Zeitspanne einer Generation zu schmelzen, so daß „lebenslanges Lernen“ und Massenarbeitslosigkeit zu üblichen Begleiterscheinungen moderner Gesellschaften geworden sind. Wer repräsentiert heute die „Internet-Generation“? Sind es die 40-

jährigen, die an der technischen Realisierung des Internet arbeiteten oder die 30-jährigen, die die ersten Gehversuche mit dem WWW machten oder die 20-jährigen, die mit Handy und Online-Zugang intellektuell in das Internet „hineingeboren“ werden. Möglicherweise sind es auch die heute erst 10-jährigen, für die Electronic Commerce eine gesellschaftlich-ökonomische Realität sein wird. Jedenfalls lassen sich „Generationen“ heute an technischen Entwicklungen festmachen, die sich binnen weniger Jahre immer wieder umwälzen. Ein Generalist wird auf seiner Abstraktionsebene in der Lage sein, bei dieser Entwicklung „auf der Höhe“ zu bleiben, während der Spezialist immer schneller gezwungen sein wird, sein Spezialgebiet zu wechseln. Im Informatik-Bereich ist die Entwicklung zum Spezialistentum – umgekehrt proportional zum Alter – am drastischsten zu beobachten: der 25-jährige ist eher in der Lage, ein technisches Problem vor dem Hintergrund aktueller Internet-Entwicklungen einzuschätzen als der 40-jährige. IT-Technik ist heute jedoch für viele Unternehmen „kriegsentscheidend“ geworden. Als Fortsetzung der Technik und der durch sie induzierten Reduktion der ökonomischen Granularität beginnen heute auch die Geschäftsmodelle, sich entsprechend umzuwälzen. Auch hier ist auf organisatorischer Ebene ein „lebenslanges Lernen“ gefragt, um nicht von den Schlaunen, Jungen überholt zu werden. Die Konnektivität des Internet spielt dabei die Rolle eines Katalysators.

- **Arbeitslosigkeit...** In ihrem Buch „Die Globalisierungsfalle“ skizzieren XXX und XXX mögliche zukünftige Gesellschaftsformen mit Arbeitslosenquoten von 30-40 Prozent und mehr – jedenfalls nach unserer heutigen Definition. Eine wesentliche Einflußgröße liegt hierbei in der schwindenden Fähigkeit des Einzelnen, sich auf dem immer schneller rotierenden Wissenskarussell zu halten. Gleiches gilt auch für Organisationen: Immer schneller vermögen daher „intelligente“ Strukturen alte und verkrustete im Wettbewerb auszuhebeln. Wenn aber durch das Internet der Wirtschaftsprozess noch weiter rationalisiert wird (z.B. durch Standardisierung, Prozeßintegration, Online-Shops), wird sich die Rolle des Menschen weiterhin weg vom Teil des Produktionsapparates hin zum Designer entwickeln. Dafür werden nach unserem heutigen Wirtschaftsmodell jedoch nur wenige benötigt: „Wirtschaft“ wird zum eigenständig rotierenden Automatismus, in den der Mensch nur zur Kurskorrektur und Beschleunigung eingreift. „Der Mensch“ entspricht hierbei aber vielleicht nur einem Fünftel der Bevölkerung. Vielleicht werden weitere zwei Fünftel für den Betrieb der physischen Ökonomie heutiger Prägung erforderlich sein; es kann aber durchaus passieren, daß die verbleibenden zwei Fünftel durch mangelnde Wissensanpassung aus dem ökonomischen Prozeß heraus-dequalifiziert werden. Nach heutiger Definition bedeutet dies Massenarbeitslosigkeit. Seit einigen Jahren befassen sich politische und gesellschaftliche Kreise wie z.B. der Club of Rome [XXX] mit diesem potentiellen Phänomen und versuchen, Gesellschaftsmodelle zu entwickeln, die eine gerechte Verteilung von „Arbeit“ anstreben. Andererseits wäre es kontraproduktiv, gerade jene intellektuellen Leistungsträger, die volkswirtschaftlich einen signifikanten Beitrag zum Bruttosozialprodukt leisten, durch Verteilungsmaßnahmen zu beschneiden. Es ist aber andererseits auch zu beobachten, daß eben diese hochgebildeten Personen sich zunehmend einen „Sabbatical“, also eine befristete „Auszeit“, aus dem Arbeitsleben genehmigen, um sich ein grundlegend neues Thema zu erarbeiten. Nicht selten wird aus dieser Ruhephase heraus der Grundstein für eine neue Produktidee oder Firmengründung gelegt.
- **... oder „Paradise Now“?** Zu beobachten ist bei der Internet-Ökonomie eine Abnahme der Bedeutung von Geld. Viele Dienstleistungen und Informationen stehen kostenlos zur Verfügung – finanziert durch Werbung und drastisch reduzierte Produktionskosten. Auch der Zugang zum Netz tendiert gegen Null: PCs werden bereits kostenlos angeboten, wenn der Käufer akzeptiert, stark personalisierte Werbeseiten anzusehen. GermanyNet et al. bieten einen kostenlosen Internetzugang an. In den USA wird der lokale Netzzugang aus Einnahmen im Fernvermittlungsbereich subventioniert. Wenn zudem auch noch im Internet Vertriebskosten wegfallen und durch effiziente Allokationsmechanismen wie Handels- oder Auktionssysteme Profitmargen minimiert werden, ist zu erwarten, daß auch Preise klassischer Produkte wie Automobile, Reisen und möglicherweise sogar Immobilien deflationieren. Technischer Fortschritt führt z.B. im Bereich der Unterhaltungselektronik seit Jahrzehnten zu kontinuierlichen Preisreduktionen. Der technische Fortschritt des Electronic Commerce spiegelt sich in Geschäftsmodellen wider, die auch in anderen Branchen zu drastischen Kosten- und Preisreduktionen führen können (siehe etwa die Beispiele weiter oben). Gesamtwirtschaftlich kann dies bedeuten, daß bei reduziertem Bruttosozialprodukt der Wohlstand dennoch wächst. Extrapoliert man diese Entwicklung, nähert man sich dem Zustand eines „Paradises“ mit kostenlosen Dienstleistungen und Produkten, aber 100% Arbeitslosigkeit [GiLe98].
- **Monopolisten ohne Zigarre.** Traditionell suggeriert der Begriff des Monopolisten das Image des bösen Raubkapitalisten, dessen Großkonzern jedem ernstzunehmenden Wettbewerber durch Übernahme oder andere Mechanismen Marktanteile entreißt. Von dieser Art Monopol ist jedoch im folgenden nicht die Rede: bizzarrerweise ist das Monopol in der Internet-Ökonomie ein erstrebenswerter Zustand, wenn es auch nicht von Dauer ist und keine Marktzutrittsbarrieren für Wettbewerber etabliert. In einer Ökonomie, die ihren Anbietern aufgrund radikalen Wettbewerbs nur kostendeckende Erträge erlaubt, verbleibt sogar im Monopol die einzige Chance, Gewinn zu generieren. Netscape war beispielsweise ein in diesem Sinne „guter“ Monopolist, da ihr gegenüber dem „Mosaic“ von der NCSA technisch verbesserter Web-Browser der einzige mit diesen Quali-

täten war. Nach einiger Zeit wurde diese Monopolstellung durch das Auftreten des Internet-Explorers von Microsoft erfolgreich angegriffen. Die kurze Monopolphase etwa um 1995/96 erlaubte es Netscape, die Rendite für die erfolgreiche Produktion und Vermarktung eines Webbrowsers einzufahren. Allgemein gesagt, kann jede Innovation somit zu einem zeitlich befristeten Monopol führen. Die Internet-Ökonomie ist folglich charakterisiert durch eine Vielzahl von Versuchen, von denen nur wenige erfolgreich enden und noch viel weniger sich zu Börsenerfolgen wie Netscape, Yahoo oder Brokat entwickeln.

Blur – oder das Verwischen bis zum Wärmetod

Alles verwischt: Rollen, Größenordnungen, Technologien, Medien, Menschen und Maschinen. Käufer verkaufen persönliche Daten, Lebensmittelhersteller kaufen Regalfläche im Supermarkt. Das Fernsehen dient als Träger von Web-Daten (URLs) und der PC wird als Internet-Fernseher eingesetzt. Spielekonsolen, die früher nur beschränkt als Universalrechner einsetzbar waren, könnten sich zum Killer entwickeln, wenn sie beim gleichem Leistungsumfang zu einem Bruchteil des PC-Preises angeboten werden. Dinge, für die man früher Geld bezahlt hat, werden kostenlos angeboten, wie z.B. PCs, bei deren Benutzung der „Käufer“ personalisierte Werbung über sich ergehen lassen muß. Dinge, die früher kostenlos waren, müssen zukünftig bezahlt werden, wie z.B. Profilinformation von Online-Teilnehmern. Unternehmen, die früher über tiefe Hierarchien und Fertigungsstufen verfügten, sind heute stolz auf die Auslagerung von so elementaren Funktionen wie Lagerhaltung, IT-Betrieb und den Verzicht auf wesentliche Bestandteile der Vertriebskette. Unternehmen atomisieren sich bis hinunter zur Einzelperson oder sie behalten ihr traditionelles Gefüge bei und schaffen interne Marktstrukturen durch das Forcieren von Profit-Centern, Gruppenentlohnung und interne Ausschreibungsverfahren. Das Unternehmen bildet dann eine juristische Hülle, innerhalb derer die externen Mechanismen des Marktes sich unverändert wiederfinden. Begriffe wie „Person“ und „Unternehmen“ verschmelzen. Schließlich stehen sich nicht mehr nur Menschen im Web gegenüber (e-Mail, Chat) oder Maschinen (Elektronischer Datenaustausch), sondern ein beliebiges Gemisch: Menschen kaufen bei Online-Shops, Softwaresysteme bestellen Ware beim Zulieferer und intelligente Agenten verhandeln mit Personen über elektronische Verträge [COSMOS XXX].

Stan Davis und Christopher Meyer haben diesem Thema ein ganzes Buch mit dem Namen „Blur“ gewidmet [DaMe98]. Nimmt man die Fülle der Beispiele für diesen Blur als Ausgangspunkt einer Entwicklung, so kann man sich das Resultat etwa so vorstellen:

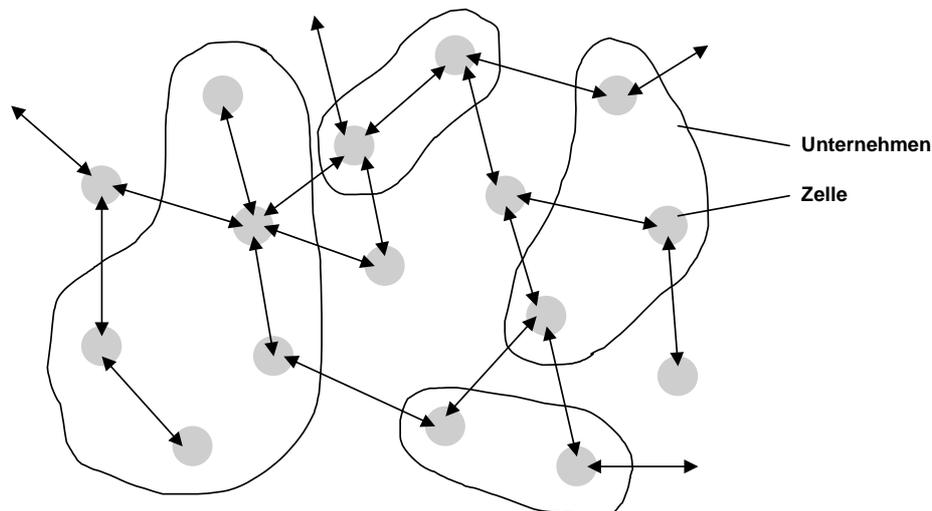


Abb. 5: Zelluläres Modell der Unternehmenskooperation

Millionen kleiner Zellen mit wenigen Mitarbeitern stellen jeweils eine operative, funktionale Einheit dar. Diese Zellen können sich leicht konfigurieren lassen. Einige dieser Zellen gehören der gleichen Organisation an; sie bilden ein Unternehmen, während sich andere Unternehmen nur aus einer Zelle zusammensetzen. Die Zugehörigkeit zu einem Unternehmen beschränkt sich auf juristische und finanzielle Aspekte, jedoch nicht auf die Aufbau- und Ablauforganisation. D.h., welche Zelle mit welchen anderen kooperiert, bleibt ihre autonome Entscheidung. Je nach Auftrag können sich dabei Ad-hoc-Zusammenschlüsse von Zellen ergeben. Ein solcher Zusammenschluß erfolgt unabhängig von der Unternehmenszugehörigkeit. Insbesondere auf der Ebene der Informationstechnolo-

gie ist das schnelle Herstellen von Interoperabilität und Kohärenz für diese flexible Kooperation erforderlich. Kooperierende Softwaresysteme müssen ad hoc konfiguriert werden können und Daten miteinander austauschen, die sie in gleicher Weise interpretieren.

Am Ende läßt sich die Unterscheidung „Unternehmen - Markt“ nicht mehr aufrecht erhalten: bereits heute werden innerhalb der Organisation Profit-Center gebildet, um mehr Entscheidungsautonomie in die Zellen zu verlagern. Eine Zelle entscheidet selbst, ob sie beispielsweise die Designabteilung des Unternehmens oder eine externe beauftragt. Damit steht die Designabteilung unmittelbar im Wettbewerb mit externen Unternehmen. Ist ein Auftrag auszuführen, tritt eine Zelle als Koordinator ein: Sie verteilt entweder den Auftrag an mehrere Subauftragnehmer und behält die Rolle des Koordinator bei oder führt lediglich Auftraggeber und Auftragnehmer zusammen. Im ersten Fall spielt diese Zelle die Rolle einer Generalunternehmerschaft, bei der eine dreistufige Hierarchie zwischen Auftraggeber, Generalunternehmer und Subunternehmern während der gesamten Abwicklung erhalten bleibt. Im anderen Fall spielt das Unternehmen lediglich die Rolle des Maklers (bzw. Brokers) und führt andere Parteien bis zur Verhandlungsphase zusammen. Für die Abwicklungsphase der Transaktion koordinieren sich Auftraggeber und Auftragnehmer anschließend selbst.

Diese Integrationsfähigkeit führt zur Bildung *virtueller Organisationen*, bei der die Unternehmenszugehörigkeit in den Hintergrund tritt und die Auftragsorientierung sowie die speziellen Kompetenzen der Partner die individuelle Konstellation einer virtuellen Organisation beeinflusst. Es wird bewußt der Begriff der virtuellen *Organisation* gewählt, da diese Kooperationsform nicht notwendigerweise nur marktorientierte Organisationseinheiten betreffen muß. Auch im universitären Forschungsbereich oder zwischen Behörden kann es prinzipiell zu einer solchen aufgabenorientierten Kooperation kommen – hierbei entfällt dann allerdings der Charakter einer Handelstransaktion, der die Grundlage für ein virtuelles *Unternehmen* (VU) bildet.

Arnold et al. definieren ein virtuelles Unternehmen als „eine Kooperationsform rechtlich unabhängiger Unternehmen, Institutionen und/oder Einzelpersonen, die eine Leistung auf der Basis eines gemeinsamen Geschäftsverständnisses erbringen. Die kooperierenden Einheiten beteiligen sich an der Zusammenarbeit vorrangig mit ihren Kernkompetenzen und wirken bei der Leistungserstellung gegenüber Dritten wie ein einheitliches Unternehmen. Dabei wird auf die Institutionalisierung zentraler Managementfunktionen zur Gestaltung, Lenkung und Entwicklung des VU durch die Nutzung geeigneter Informations- und Kommunikationstechnologien weitgehend verzichtet“ [AFHS95].

Folgende Kriterien werden als Voraussetzung für virtuelle Unternehmen angeführt:

- Das VU ist eine Kooperation von Unternehmen. Diese können allerdings zwischen Einzelpersonen und Großunternehmen variieren.
- Die involvierten Unternehmen behalten ihre ökonomische und juristische Selbständigkeit bei. VUs sind damit keine Joint-Ventures, eher Gesellschaften Bürgerlichen Rechts (BGB-Gesellschaften). Damit können sich verschiedene Probleme bei internationalen VUs ergeben (vor allem die Frage des Gerichtsstands).
- Der Zweck des VU liegt in der optimalen Nutzung von Kombinationsmöglichkeiten und Ressourcen, die intern nicht zur Verfügung stehen.
- Eine VU ist für beliebige Unternehmen offen, die eine erforderliche Resource zur Verfügung stellen können.
- VUs werden aufgelöst, sobald der Zusammenschluß nicht mehr erforderlich ist (z.B. nach Ablauf eines Projekts).
- VU können sowohl horizontale als auch vertikale Kooperation erfordern (mehrere Unternehmen innerhalb einer oder mehrerer Branchen).
- VUs besitzen keine hierarchische Struktur. Es existiert kein weisungsbefugter Partner oder Subauftragnehmer.
- Vertrauen gilt als das wichtigste Bindungsmerkmal zwischen den Partnern des VU.

Abb. XXX zeigt die beteiligten Teilnehmer einer virtuellen Organisation am Beispiel einer Buchpublikation. Hierbei stehen Dienstleister wie Werbeagenturen, Korrekturleser, Tiltelbild-Designer, Bibliotheken, Druckereien usw. bereit, um einen Teil des gesamten Publikationsprozesses zu übernehmen. Der Autor übernimmt hierbei (im Gegensatz zum herkömmlichen Modell) die Rolle des Auftraggebers. Da die Koordination aller erforderlichen Dienstleistungen für den Autor selbst zu komplex ist, beauftragt er einen Experten, der diese Tätigkeit so oft ausübt, daß er nicht nur in der Lage ist, die erforderlichen Services zu koordinieren, sondern auch die für diesen Auftrag speziell geeigneten zu ermitteln. Gegenüber dem Auftraggeber bietet der Publikationsagent eine einheitliche Schnittstelle, über die eine Auftragsvergabe erfolgt sowie der Austausch des Manuskripts.

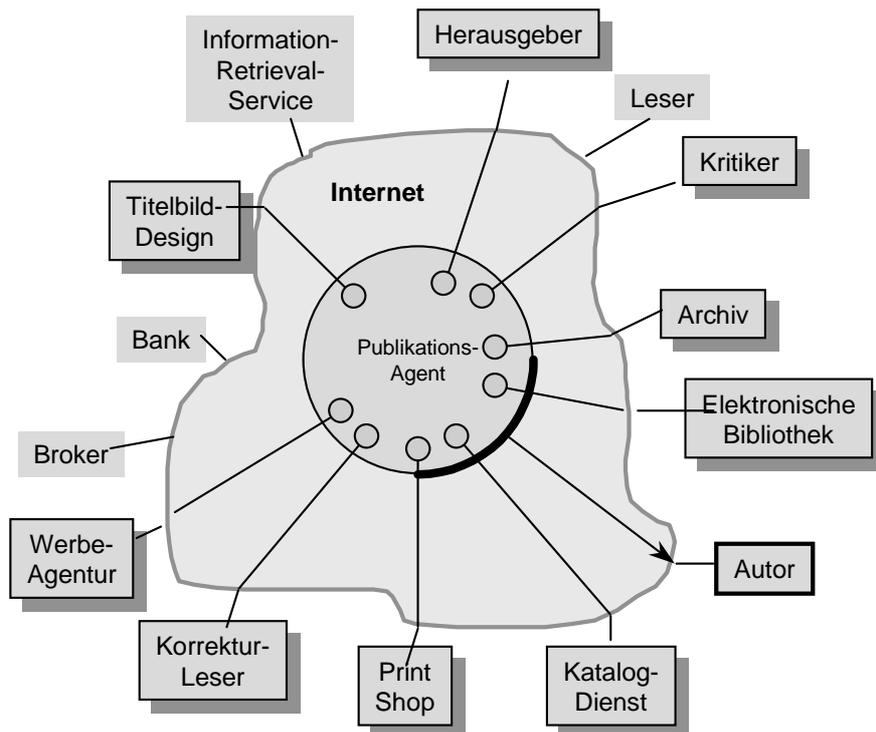


Abb. 6: Beispiel für ein virtuelles Unternehmen

Neben der Aufbauorganisation kümmert sich der Generalunternehmer um die Ablauforganisation. Dabei werden einzelne Prozesse der Partner so miteinander integriert, daß der Gesamtauftrag unter Berücksichtigung der Abhängigkeiten einzelner Aktivitäten in kürzester Zeit abgewickelt werden kann. Dies führt zu einem organisationsübergreifenden Workflow, dessen prinzipielles Schema mit immer wieder neuen Partnern angewendet werden kann. So können wir annehmen, daß der Agent nach Vertragsabschluß mit dem Autor dessen Manuskript erhält und dieses weiterleitet an den Korrekturleser und den Titelbilddesigner. Er selbst erstellt ein Abstract, das für den Katalogdienst, aber auch als Grundlage für die Werbeagentur verwendet wird. Das Manuskript wird nach der Korrektur an den Autor zurückgeliefert. Evtl. kann sich der Korrekturzyklus mehrfach wiederholen. Schließlich wird jedoch die endgültige Fassung an den Print Shop geliefert und gedruckt.

In der Praxis wird eine solche Vorgehensweise bereits heute bei Kleinunternehmen in der Baubranche, bei Werbeagenturen oder auch Softwarefirmen praktiziert. Bei größeren Unternehmen ist meist ein erheblich höheres Auftragsvolumen erforderlich, bis es „sich rechnet“, sich in dieser Form in einen Verbund zu integrieren. Es sei denn, kleinere flexible Einheiten, die autonome Entscheidungen treffen können, werden aus dem Großunternehmen in die virtuelle Organisation einbezogen – dann finden wir wieder die oben illustrierte Zellenorganisation vor.

Bis zum Wärmetod?

Der zweite Hauptsatz der Thermodynamik besagt, daß – in kosmischen Größenordnungen gemessen – jegliche Materie zu einer diffusen, strukturlosen Masse mit maximaler Entropie verschmilzt, deren Bestandteile keinerlei Energiedifferenz und damit auch keinerlei Information besitzt. Angewendet auf die Zellenorganisation, bedeutet dies, daß ein Unternehmen befürchten muß, sein spezielles Profil zu verlieren, wenn seine Bestandteile vergleichbar werden mit denen seiner Wettbewerber. Ohne Profil droht die Zelle und das Unternehmen jedoch in einem Meer vergleichbarer Zwillinge unterzugehen. Folglich ist ein Vehikel erforderlich, daß nicht nur Aufmerksamkeit bei Geschäftspartnern oder Konsumenten erzeugt, sondern bestimmte Qualitäten markiert. Dieses Vehikel ist der Markenname, hinter dem alle Zellen des Unternehmens organisiert werden können. Ein Softwareunternehmen, das als Tochter der Lufthansa AG denselben Namen tragen darf, erhält im Ausland bereits einen Aufmerksamkeitsbonus. Gleiches gilt für Banken, Automobilhersteller, Lebensmittelkonzerne und andere Markenartikler. Von einem Unternehmen „Porsche Software Design“ würde man beispielsweise hohe Ansprüche an Qualität und Design erwarten. Gerade die Marke bietet in der Internet-Ökonomie die Möglichkeit, einen Fixpunkt zu markieren im Rauschen der Home-Pages und Web-Links.

Meta-Organisationen und ihre Software

Durch steigende Dominanz des Marktprinzips gegenüber dem Planungsprinzip gewinnt das Chaos und verliert die Struktur. Damit steigt die Geschwindigkeit, mit der eine Struktur etabliert werden und auch wieder zerfallen kann. Die Komponierbarkeit dieser Struktur hängt jedoch stark von der Verfügbarkeit ihrer Bestandteile ab: Während eben früher ein PC weitgehend von einem Unternehmen geplant, gefertigt und montiert werden konnte, bestand die Übergangsphase in der Beauftragung von Zulieferern zu Herstellung der Komponenten. Heute besteht ein derartig hohes Standardisierungsniveau, daß Komponenten und deren Montage auf hochtransparenten Märkten bei nahezu gewinnlosen Margen von wechselnden Herstellern eingekauft werden können.

Unternehmen, die in der Internet-Ökonomie bestehen wollen, sind also auf neue, netzartige Strukturen angewiesen. Um ein solche Struktur zu realisieren, muß sich das Management einerseits traditioneller Instrumente wie Fusionen, Übernahmen und Joint Ventures bedienen, andererseits kommen neue Formen der Kooperation mit jungen Start-Ups hinzu, die mit Hilfe von Risikokapital übernommen werden. Einige Unternehmen wie beispielsweise XXX (seit 1998 am Neuen Markt) leben zum größten Teil davon, daß sie das durch Aktienemissionen verfügbare Kapital in Unternehmensaufkäufe investieren, um aus der möglichen Synergie der Beteiligungen einen Mehrwert zu schöpfen. Solche Unternehmen sind bereits heute hochvernetzte Strukturen, die nicht mehr auf der Basis eines autokratischen Führungsstils, sondern durch Einflußnahme und Überzeugung geführt werden. Ein Unternehmer ist damit nicht mehr nur Architekt eines spezifischen Aufbau- und Ablaufmodells seiner Organisation, sondern „Meta-Architekt“: Er muß eine Infrastruktur schaffen, die ihrerseits das Aufbauen und Zum-Ablauf-Bringen der Zellen erleichtert. Diese Meta-Architektur erstreckt sich von der Organisation bis hin zur IT-Infrastruktur. Auf beiden Ebenen gilt es, schnelle Verbindungen zu knüpfen, neue Zellen rasch etablieren oder auch terminieren zu können und dies 1:1 durch Softwarekomponenten zu reflektieren.

Zu unterscheiden ist speziell im Hinblick auf virtuelle Organisationen die Kooperation auf rein organisatorischer Ebene (heute bereits der Fall) und die Integration der beteiligten IT-Systeme. Im letzteren Fall ist eine Reihe von Anforderungen zu erfüllen:

1. **Interoperabilität.** Diese elementare Anforderung zielt auf die technische Integration der beteiligten Kommunikationsdienste ab. Dabei sind Verfahren erforderlich, die den Transfer von Daten zwischen Rechnern auf der Basis standardisierter Protokolle unterstützen, die Lokalisierung von Softwarekomponenten sowie die korrekte Bindung der jeweils erforderlichen Komponenten. Diese Anforderungen werden von Middleware-systemen wie CORBA, DCE oder verteilten Java-Systemen (Voyager, RMI) erfüllt. Stellvertretend werden dazu im Kapitel XXX einige Grundlagen von CORBA erläutert.
2. **Semantische Kohärenz der Daten.** Hierbei geht es nicht nur darum, Datenwerte entsprechend ihrer Typen zu übertragen, sondern ihre einheitliche Interpretation zu forcieren. Erforderlich ist dazu die Standardisierung von Semantik: d.h. „RENr“ ist nicht nur eine natürliche Zahl, sondern als Rechnungsnummer zu interpretieren. Bereits seit Jahrzehnten werden solche Informationen für den elektronischen Datenaustausch im Rahmen von EDI-Standards normiert, jedoch ergeben sich immer wieder organisatorische Schwierigkeiten beim Standardisierungsprozeß, so daß in der Realität die meisten EDI-Nachrichten inkompatibel sind und nur mit hohem Aufwand konvertiert werden können.
3. **Workflow-Steuerung.** Isolierte Informationstransfers sind im Zusammenhang von Geschäftsprozessen zu koordinieren. Die Reihenfolge solcher Nachrichten, Verzögerungen und Fristen, Ausnahmesituationen und Regeln sowie die hierarchische Zusammenfassung einzelner Prozesse zu verdichteten Abläufen sind die Aufgabe von Workflow-Management-Systemen. Nur wenn ein solcher Prozeß beschrieben werden kann, besteht auch die Chance, in der virtuellen Organisation eine sinnvolle Verteilung der Subaufträge vorzunehmen.
4. **Juristische Absicherung der Leistungen.** Da bei jeder Kooperation zwischen dem Publikationsagenten und einem Geschäftspartner ein Austausch von Leistungen steht, zu dem beide Parteien eingewilligt haben, liegt jeweils ein Vertrag vor. Dieser könnte abstrakt als mündliche Vereinbarung existieren oder als elektronisches Dokument. Zur beweisfähigen juristischen Absicherung der Leistung ist jedoch der Einsatz elektronischer Signaturen sowie die Sicherung des Dokuments erforderlich. Diese Thematik wird im Kapitel XXX unter dem Thema „Electronic Contracting“ behandelt.
5. **Datenschutz.** Diese Form von Datenschutz betrifft im Falle virtueller Organisationen die lokale Information eines Partner-Unternehmens, das seine lokale Information vor dem Zugriff der Geschäftspartner sichern will. Beispielsweise gilt für Verträge, die der Publikationsagent mit seinen Geschäftspartnern geschlossen hat: Weder sollen die Subauftragnehmer Einblick in den Vertrag mit dem Autor gewinnen noch umgekehrt.

Wenn Partner dabei immer neue Kooperationen eingehen, so erfordert dies flexible IT-Systeme zur schnellen Anpassung. Erforderlich sind dazu Systeme mit standardisierten Softwareschnittstellen, die sich ad hoc zusammenschalten lassen. Verändert ein Unternehmen seine Kooperationsbeziehungen; muß es möglich sein, diese Beziehung auf der Softwareebene unmittelbar nachzuführen. Um diesem hohen Anspruch gerecht zu werden, ist

es erforderlich, moderne Softwaretechnologien wie Komponenten, Frameworks und Business Objects einzusetzen (siehe dazu Kapitel XXX).

Mega-Unternehmen oder Micro-Enterprises

Die 200 größten weltweit agierenden Unternehmen erzielen bereits einen Umsatz, der höher als ein Viertel des gesamten Welthandels ist; und sind größer als viele Volkswirtschaften; sie beschäftigen dabei allerdings nicht einmal ein Prozent der arbeitsfähigen Menschen. Philip Morris etwa ist bez. des Umsatzes größer als Neuseeland, Mitsubishi ist größer als Indonesien, General Motors größer als Dänemark oder Toyota größer als Norwegen. 51 der hundert größten Wirtschaften sind Unternehmen. Wenn man von den neun größten Volkswirtschaften absieht (USA, Japan, Deutschland, Frankreich, Italien, Großbritannien, Brasilien, Kanada und China) übertrifft der Umsatz der 200 größten Unternehmen weltweit das gemeinsame Bruttosozialprodukt aller verbleibenden 182 Länder.

Folglich muß man sich fragen, ob für ein Unternehmen in Zukunft die schiere Größe oder die flexible Zelle anzustreben ist. Im Prinzip schließen sich diese Ansätze nicht aus, denn die meisten Großunternehmen werden heute als dezentralisierte Bündel relativ autonomer Zellen geführt. Durch Instrumente wie Profit-Center oder Gruppenentlohnung wird die Gewinnverantwortung bis in einzelne Arbeitsgruppen hinein verlagert. Jede dieser Zellen kann im Extremfall frei entscheiden, ob erforderliche Dienstleistungen aus der Organisation heraus oder von Dritten bezogen werden sollen. Am Ende erscheint die Trennlinie zwischen dem Mega-Unternehmen und dem Micro-Enterprise so dünn wie die Linie der Unternehmensgrenze in Abb. XXX.

4.2.2 The Winner takes it all...

Neben der euphorischen Einschätzung, daß das Volumen des Electronic Commerce sich auch in den nächsten Jahren explosionsartig ausweiten werde, existieren einige kritische Stimmen, die darauf hinweisen, daß das größere Volumen nicht zwangsläufig zu einer Vergrößerung der Zahl an Online-Anbietern führt. Der einfache Grund liegt in der begrenzten Aufnahmefähigkeit der Benutzer. Abgesehen davon, daß das Internet selbst mit anderen Medien wie Fernsehen und Print-Produkten konkurriert, ist die Aufmerksamkeit für eine beliebige Anzahl Anbieter in einem bestimmten Marktsegment begrenzt: Alle kennen Amazon.com, einige kennen vielleicht noch Barnes and Noble und BOL. Wer aber kennt Libri oder Buch.de? Und all die anderen Online-Buchhändler, die ich selbst nicht kenne, daher hier auch nicht auflisten kann? Und wer hat wirklich mehr als ein, zwei Online-Bookshops benutzt? Ich selbst nur Amazon.com. Für einen zweiten gibt es fast schon keinen Platz mehr, spätestens der fünfte kann nur überleben, wenn er subventioniert wird. Grob geschätzt gilt dieses Verhältnis langfristig für alle Märkte – Autos, Immobilien, Portal-Sites, Suchmaschinen etc.

Das Modell dahinter kann als „The-winner-takes-it-all-Ökonomie“ charakterisiert werden. Nur ein Mitspieler – meistens der erste am Markt – ist in der Lage, durch einen Zeitvorsprung von oft nur wenigen Monaten, seine Online-Community und sein Angebot soweit zu vergrößern, daß es jederzeit im Vergleich zum zweiten bei weitem attraktiver wirkt. Unternehmen wie Intershop, Brokat, Amazon oder Yahoo haben nur ein kurzfristiges Ziel: einen konstanten Marktanteil bei explodierendem Marktvolumen zu halten. Darum muß mehr als der Gewinn hergibt in die erforderliche Expansion investiert werden. Bei Intershop sind dies etwa 10% Weltmarktanteil. Würde Intershop sich plötzlich entscheiden, nicht mehr diesen Anteil zu halten, ist eine erhebliche Gewinnmarge zu erwarten. Da jedoch international nur die ganz wenigen Großen einer Branche langfristig Überlebenschancen haben, investieren sie unvorstellbare Summen, nur um ein Wachstum zu sichern, das mindestens dem des Marktes entspricht. So hatten sich AOL und Sun den Erwerb von Netscape XXX Milliarden Dollar kosten lassen. Yahoo zahlte XXX Milliarden für die Akquisition von GeoCities und XXX für XXX.

Was bedeutet diese Entwicklung nun langfristig? Es kann passieren, daß in gewissen Märkten, nach der Bereinigung und Akquisitionswelle, eine neue globale Monopolisierung stattfindet, d.h. nur wenige große Anbieter werden ihren jeweiligen Markt beherrschen. [XXX McGovern und der Internet Retailing Report]

4.2.3 Vertrauensökonomie

„Alles hat seinen Preis“

Wie bereits bei der Payment-Klassifikation angedeutet, kann man Faktoren wie "Sicherheit" und "Vertrauen" einen Wert beimessen, der in einem gesunden Verhältnis zum Transaktionsvolumen stehen sollte. Es macht keinen Sinn, einem Notar 500,- DM zu zahlen, nur um den Kauf eines Paar Socken zu beurkunden. Umgekehrt läßt man sich den Zahlungstransfer eines Kunden aus einem finanziell instabilen Land durch komplizierte Akkreditivverfahren etwas mehr kosten, wenn dadurch sichergestellt ist, daß die unwiderruflich versendeten Güter nicht zum Ruin der Firma führen.

Vertrauensökonomie bedeutet auch, daß sich Bürger eines Weichwährungslandes "harte Dollars" zulegen, um mögliche Abwertungsrisiken zu vermeiden. Die Mehrkosten des erforderlichen Devisenumtausches nehmen sie dabei in Kauf.

Im Internet kann eine mangelnde Vertrauensinfrastruktur (bis heute glücklicherweise nur theoretisch) zu Micro-Payment-Raubrittertum führen, wenn sich nämlich ein Mitarbeiter eines Online-Anbieters wie Amazon.Com plötzlich entscheidet, nur die einfließenden Millionenbeträge eines einzigen Tages auf die Cayman-Islands zu überweisen und selbst gleich hinterherzufliegen.

Heute ist noch unklar, ob sich das Rad des Zahlungs- und Warenumschlags beim Internet-Commerce einfach nur schneller drehen wird, oder ob es zu qualitativ neuartigen Prozessen kommen kann, die heute noch nicht zu extrapolieren sind.

Jedenfalls kann aus der Erfahrung mit der Beschäftigung rund um den Electronic Commerce nur konstatiert werden, daß im praktischen Einsatz Fragen auftreten wie: "An wen kann sich XXX wenden, wenn YYY passiert", "Woher nimmt AAA die Sicherheit, BBB zu tun", "Wie bekommen wir möglichst viele MMMs ins Boot, damit unsere NNNs uns abkaufen, daß wir OOO sind" usw. Weniger drängend ist danach die zu klärende technische Umsetzung des Ganzen.

Da uns die technische Infrastruktur des Internet eine weitreichende Formalisierung von Dingen aufzwingt, die wir vorher eher auf die "weiche" Art lösen konnten, stehen wir vor neuen Problemen. Vorher signalisierte uns das 20 Meter hohe Marmorportal der Bank, daß es ihr eigentlich gar nicht finanziell schlecht gehen kann. Oder der weißbekittelte Arzt mit dem grauen Haaransatz, der sonoren Stimme und dem beruhigenden Titel suggerierte uns, daß er eigentlich keinen Kurpfusch begehen kann (und in diesem Glauben werden wir wohl auch umso gesünder ;-). Aber ach, im Internet ist alles auf 1024x768 Pixel normalisiert. Dort befindet sich das ach so dominante Pornoprogramm direkt neben unserem Gesundheitsberater und beide sind über die www.cybermall.tv erreichbar, die mit der www.clearmoney.tm kooperiert. Weder wissen wir, wo sich der Firmensitz dieser Unternehmen, noch der des ISP befindet. Einzig erkennbar ist, daß sich die Toplevel-Domains in Tuvalu respektive Turkmenistan befinden.

In der synthetisierten Welt des Internet-Marktes besteht also ein sehr wohl nachvollziehbarer Bedarf an vertrauensschaffenden Maßnahmen. Leider kostet dies Geld. Daher wird es wohl zukünftig eine Vertrauensdiversifikation geben, deren Spektrum von

<Vertrauen=0 UND Risikobereitschaft=0>

reicht bis zu

<Vertrauen=max. UND Risikobereitschaft=max.>.

Dieses Kontinuum ist begleitet von wachsenden Kosten hin zur ersten Ausprägung. Die Quantisierung des Kontinuums erinnert einen an die erste Frage des Sparkassen-Beamten bei der Anlageberatung, ob man an einer spekulativen oder konservativen Strategie interessiert ist. Damit wird in seinem Kopf zunächst erst einmal ein großer "Radio-Button" betätigt, der eine von drei Kategorien festlegt. Alles weitere ergibt sich dann aus den Anlageempfehlungen des Computers.

Eine derartige Formalisierungsstufe ist im Internet nicht gegeben. Immerhin gibt es einige freiwillige Bestrebungen zum Selbst-Rating (siehe auch Abschnitt XXX), das heute jedoch weder interoperabel noch verbindlich und damit "einklagbar" ist. Denn nur, wenn ich nachweisen kann, daß ich eine konservative Anlagestrategie verfolge und mir dennoch eine Ramschanleihe verkauft wurde, besteht für mich überhaupt ein Ansatzpunkt für den juristischen Hebel. Ich persönlich glaube andererseits, daß ein hierzu offiziell autorisierter "Internet-Rating-Großer-Bruder" nicht viel mehr nützen wird als die Übertragung des Vertrauens in real existierende Institutionen in das Netz. Wenn die Deutsche Bank eine Online-Mall betreibt, dann vertraue ich ihr genauso wie ich ihr vertraue, wenn meine DB-Aktien fallen, da sie sich in irgendwelchen Finanztransaktionen verspekuliert hat. Es gibt niemals eine risikofreie Welt, die bezahlbar ist. Ich vertraue der Bank allerdings mehr als dem XYZ-Provider in Blauland. Und dem UVW-Betreiber in Blauland vertraue ich mehr als XYZ, da er mit der Deutschen Bank ko-

operiert und ich davon ausgehen kann, daß die sich um ihres guten Rufes willen nicht blamieren will.

Ein etabliertes System, Vertrauen zu schaffen, ist die Marke. Markennamen sind Leuchtfeuer für Konsumenten, die durch das Dickicht unbekannter Web-Seiten stochern. Markennamen helfen einem Unternehmen, sich ein wenig aus einem Wettbewerb herauszuhalten, der ausschließlich über den Preis geführt wird. Eine Marke besitzt daher kaum meßbaren Wert, der sich in Folge einer Tradition der Zuverlässigkeit aufbaut. Die schwierigste Aufgabe für den Neustart eines Unternehmens im Internet ist folglich die rasche Einführung und Etablierung eines Markenzeichens. Aus diesem Grunde ergeben sich üblicherweise Allianzen aus Reputationsspendern und Empfängern, das sich heute noch nicht präzise quantifizieren läßt.

Eines ist jedoch sicher: "Vertrauen schaffen" wird ein zukünftiges Geschäft im Internet. Mögliche Branchen sind hierbei "elektronisch verlängerte" Notare, Rating-Agenturen, alle Unternehmen, die in der realen Welt einen hohen Vertrauensvorschuß genießen, aber auch Nationalstaaten und nichtkommerzielle Institutionen, für die dieses gilt. Neben diesen "optimistisch motivierten" Institutionen sind umgekehrt allerdings auch Institutionen denkbar, die in Erscheinung treten, nachdem es zum Delikt kam: Rechtsanwälte, Gerichte, Detektive. Wie diese im Internet agieren können, sei der Phantasie des Lesers überlassen.

Ebenso wie Ökonomen argumentieren, daß in einem globalisierten Markt mit freier Mobilität der Wirtschaftsfaktoren die Rolle des Nationalstaates sich in der Schaffung und Erhaltung allgemeiner "Sicherheit" konzentriert, so kann dies auch für Organisationen gelten. Heute vertrauen wir auch kleinsten Organisationen, daß sie *ihre spezielle* Aufgabe korrekt leisten: Die Object Management Group (OMG), eine Organisation mit ca. 15 Mitarbeitern standardisiert die Common Object Request Broker Architecture (CORBA). Dies kann nur erfolgen, wenn die über 600 Mitgliedsorganisationen in diese Fähigkeit zur korrekten Koordination vertrauen. Platzt dieses Vertrauen, dürfte eine solche Organisation über Nacht aufhören zu existieren. Gleiches gilt für Unternehmens-Rating-Agenturen wie Moody's und Standard & Poors, die Stiftung Warentest oder den Universtäts-Professor, der für Gutachtertätigkeiten herangezogen wird.

Ein Beispiel für das Modell "Vertrauen in eine respektierte Organisation" ist T-Online (bzw. früher BTX) der Deutschen Telekom. Ihre Mitarbeiter *könnten* Transaktionen zu eigenen Gunsten im Namen und auf Rechnung von Kunden durchführen, aber dies ist – obwohl bereits vorgekommen – so marginal, daß sich kaum ein T-Online-Kunde (berechtigterweise) Gedanken darüber macht. Jeder Beteiligte rechnet sein Risiko in "seinen" Preis hinein: Die Telekom kalkuliert dies in ihren Gebühren und der Kunde in seinem Zeitbudget – evtl. muß er sich einmal im Monat 10 Minuten Zeit nehmen, um den seltenen Fall aufzudecken, daß ein nicht autorisierter Betrag abgebucht wurde. Aber dies gilt nur unter folgenden Voraussetzungen:

1. Jeder Beteiligte ist sich seines Risikos quantitativ bewußt.
2. Im Falle eines Fehlers muß der Beweispflichtige definiert und eindeutig erkennbar sein.
3. Die Schuldverteilung muß fair sein.

Wenn diese Voraussetzungen (und verschiedene, daraus ableitbare) nicht bei allen Geschäftsbeziehungen erfüllt sind, kann nicht von einem "fairen" Risiko ausgegangen werden. Es kann dem Anleger nicht mehr die Einhaltung der konservativen Anlagestrategie zugesichert werden. Vielmehr ginge das "Business-Modell" von einem Pionier-Unternehmer mit Goldgräber-Mentalität aus – dies paßt jedoch nicht zu den meisten von uns. Infolge dessen scheint hier ein dosierter, aber wirkungsvoller staatlicher Eingriff in den elektronischen Markt durchaus wünschenswert.

4.2.4 „Vollkasko-Wirtschaft“ vs. „Free-Economy“

Zur Zeit sind zwei gegenläufige Trends zu erkennen: Die „wasserdichte“ Ökonomie und die laissez-faire-Ökonomie. Die wasserdichte ist vollständig reguliert, es wird mit nicht-anonymen Geldkarten bezahlt, die einerseits Banken die Erstellung eines Bewegungs- und Kaufprofils erlauben, andererseits jedoch die Wiederherstellung des elektronischen Portemonnaies ihrer Kunden. In der wasserdichten Wirtschaft sind alle Rechtsituationen beim elektronischen Handel eindeutig bekannt und supranational harmonisiert. Die wasserdichte Ökonomie ist teuer, aber sicher: überall fallen Buchungen und Belege an, die gesetzesmäßig auf Jahre zu archivieren sind; es existiert nur die eine von der Notenbank herausgegebene Währung und strenge Daten- und Verbraucherschutz-Regelungen definieren exakt, in welchen Fällen welche Informationen zwischen wem ausgetauscht werden können. Handelstransaktionen erlangen nur Gültigkeit, wenn sie sich in einem archivierbaren Vertrag niederschlagen. Die nationale Notenbank ist ausschließlich für den Umlauf und die Steuerung einer einzig zulässigen Währung verantwortlich.

Die Free-Economy hingegen ist billiger, riskanter, aber auch flexibler: Transaktionskosten fallen so gut wie gar nicht an, da keine Verpflichtung zu kostspieligen Buchungsvorgängen besteht. Statt dessen helfen kryptographi-

sche Verfahren, wie sie beispielsweise bei Ecash angewendet werden, zur Sicherung des Bargeldes gegen Fälschung. Geschäfte durchzuführen ist in der Free-Ökonomie grundsätzlich riskanter, aber das Risiko wird durch die niedrigen Transaktionskosten ausgeglichen. Mehrere Währungen stehen im Wettbewerb und diese werden von Nicht-Notenbanken herausgegeben. Im Währungswettbewerb konkurriert der Gates-Gulden mit dem Telekom-Taler und ihr Wechselkurs kann sich täglich ändern. Er drückt das Vertrauen in den Herausgeber aus, d.h. nur extrem vertrauenswürdige Organisationen werden von den Wirtschaftssubjekten überhaupt als „Notenbank“ akzeptiert. Auch Banken beliebiger dritter Staaten können sich am Privatwährungswettbewerb beteiligen, dagegen kann in Ländern mit verordneter wasserdichter Wirtschaft zunächst niemand etwas ausrichten. In der Free-Ökonomie kann jeder Teilnehmer zu jedem Zeitpunkt einen Shop, eine Bank oder sogar eine Notenbank eröffnen. Markttransparenz wird durch Dienste geschaffen, die als Rating- oder Suchmaschinen von jedem genutzt werden können. Die Free-Ökonomie setzt keine Verordnungen zur Steigerung der Sicherheit voraus: Mehr technische Sicherheit kostet mehr Geld und verzögert geplante Aktivitäten (einen Kauf, die Einrichtung eines Shops oder einer Bank). In der Free-Ökonomie existieren keine Markteintrittsbarrieren – jeder darf alles. Allerdings wird der drohende Verlust an Reputation, die ein Teilnehmer am Markt gewonnen hat, jeden motivieren, unsichere oder gar kriminelle Verhaltensweisen zu vermeiden. Anstelle der staatlichen und technischen Kontrolle tritt die soziale bzw. marktwirtschaftliche.

Beide Ökonomien können natürlich parallel existieren, sie stehen sogar im Wettbewerb. Daher muß man sich als Marktteilnehmer entscheiden, welches Geschäft man in welchem Kontext abwickeln will. Die Wahl der Internet-Ökonomie entspricht damit dem Gang zum Anlageberater bei der Sparkasse: bevor man eine Anlageempfehlung erhält, erfolgt zunächst eine Klassifikation der eigenen Anlagestrategie. Ist diese konservativ (wasserdichte Wirtschaft), liefert der Sparkassencomputer eine Reihe risikoloser, sicherer, aber auch wenig rentabler Anlageempfehlungen. Im anderen Fall muß sich der spekulative Anleger auf mitunter recht waghalsige Investments einlassen.

Ein interessantes Stichwort zur Free-Ökonomie lautet „Soziale Kontrolle“: Nur wenn für jeden Marktteilnehmer ein Anreiz besteht, sich fair zu verhalten und dieses Verhalten Voraussetzung für profitable Geschäfte ist, kann sie florieren. Die Bank wird es sich genauso wenig leisten wollen und können, aufgrund unzuverlässiger Online-Shops, die von Dritten über die Bank-eigene Mall betrieben werden, beim Kunden in Mißkredit zu geraten. Folglich wird die Bank im Rahmen des Möglichen versuchen, solche Fälle auszuschließen und ein geeignetes Frühwarnsystem zu installieren.

...

Welches der beiden dargestellten Modelle sich am Ende durchsetzen wird, ist in keiner Weise abzusehen. Zunächst wird der aktuelle Zustand der Rechtsfreiheit in einigen Bereichen wohl noch anhalten, allerdings ohne der radikalen Deregulierung der Free-Ökonomie nahezukommen. Im Laufe der Zeit dürften die Regulierer Oberhand gewinnen und Rechtssituationen der wasserdichten Wirtschaft Schritt um Schritt festlegen und standardisieren können. Gleichzeitig jedoch kann sich durch eine Graswurzelbewegung die Free-Ökonomie unter Umgehung des staatlichen Einflusses der wasserdichten Wirtschaft Raum verschaffen.

...

4.2.5 Netzwerkexternalitäten

Externalitäten sind „Abfallprodukte“ von Handelstransaktionen, die nicht in der Buchführung der beteiligten Unternehmen erfaßt sind. So ist die Umweltbelastung einer Chemiefabrik ein externer Effekt oder der Parkplatz am Einkaufszentrum, der am Wochenende kostenlos für Flohmärkte zur Verfügung steht.

Eine (positive) Netzwerkexternalität ist dann gegeben, wenn eine Transaktion nicht nur den unmittelbar Beteiligten zugute kommt, sondern nebenbei eine Gemeinschaft vergrößert, die von der zunehmenden Größe profitiert. Als Paradebeispiel wird meistens die Einführung von Faxgeräten angeführt: Die ersten beiden Fax-Benutzer nützen noch niemandem außer sich selbst (der erste sogar nicht einmal sich selbst!). Sobald jedoch weitere Mitglieder zur Gemeinschaft der Fax-Nutzer hinzukamen, wurde das Medium Fax auch für alle existierenden Nutzer immer attraktiver. Das gleiche gilt für das Internet, das WWW, Microsoft Word, SAP usw.

Ein Wirtschaftsverband kommerzialisiert Netzwerkexternalitäten durch die zunehmende Vermaschung von Geschäftsbeziehungen und Wissen. Hier bei wird die positive Netzwerkexternalität durch Mitgliedsbeiträge monetarisiert.

Das Austauschen von Wissen ist ein gesamtgesellschaftlicher Effekt, der erst durch das Internet in radikaler Weise vorangetrieben werden konnte. Innerhalb der gesamten Internet-Gemeinde versuchen nun Anbieter Netzwerkexternalitäten für sich zu nutzen, indem sie die Attraktivität der von ihnen verwalteten Community steigern und

ebenso ihre Werbeeinnahmen. Damit wird auch dieser sonst nicht erfaßte externe Effekt ein kommerzialisierbares Gut. Diese Aussicht auf Gewinn hat letztlich ein völlig neues Marktsegment der Community-Verwalter begünstigt.

4.2.6 Free Economy: Kein Umsatz ohne "Teaser"

Im Internet verliert Inhalt an Wert. Egal ob im Musik-, Software- oder im Textbereich – Kopieren ist immer noch am billigsten. De-facto kann davon ausgegangen werden, daß im Softwarebereich die Dunkelziffer bei XXX% des Umsatzvolumens liegt (PC-Standardsoftware). Ähnliche Entwicklungen zeichnen sich heute bereits im Musikbereich ab, und wenn Bücher elektronisch vertrieben werden, wird sich diese Entwicklung erneut wiederholen. Es gibt ohnehin genug Anbieter im Netz, die für ihre Inhalte nichts berechnen. Für einige besteht die Hoffnung, damit Aufmerksamkeit auf ihre Lyrik oder Fotos lenken zu können, für die meisten anderen spielt das kostenlose Internet-Angebot die Rolle eines Appetithäppchens, mit dem ein potentieller Kunde geworben werden soll. Dabei handelt es sich nicht nur um Produktfragmente wie z.B. Inhaltsverzeichnisse von Büchern (XXX Link auf dieses Buch bei Ponton), sondern um vollwertige und funktionsfähige Produkte.

Mit dem Teaser-Angebot werden jedoch trotz allem ökonomische Ziele verfolgt: Zunächst dient es der Kundenbindung. Wie z.B. bei www.mietshop.de praktiziert, wo man als zukünftiger Shop-Betreiber für einen Monat seinen Online-Shop in der MietShop-Mall kostenlos betreiben kann. Die Überwindung, nach mühseliger Kleinarbeit den Shop wieder abzubauen, ist dann recht groß. Ein weiteres Ziel ist jedoch die Erlangung von Aufmerksamkeit für den Anbieter. Jemand, der als Autor eines Linux-Treiber Ruhm und Ehre erlangt, wird eher von Auftraggebern nachgefragt, als ein „unbeschriebenes Blatt“. Im Gegensatz zum „Inhouse-Entwickler“ beim Softwareunternehmen erlangt der „Linux-Entwickler“ unmittelbare Sichtbarkeit am Markt. Damit sind wir wieder bei der e-Lance-Ökonomie angekommen, die durch frei handelnde Einzelpersonen geprägt ist. Um jedoch nicht in einem Heer der Einzelkämpfer unterzugehen, muß Aufmerksamkeit erlangt werden. Dies ist jedoch nicht mit „Reklame“ gleichzusetzen, da sich der Aufmerksamkeitsmechanismus der Free Economy auf der inhaltlichen Ebene abspielt: das Softwareprodukt wird kostenlos angeboten, um am „Customising“ zu verdienen. Da die Zahl der kostenlosen Produkte wächst, entsteht zusätzlicher Preisdruck auf die traditionellen Softwareanbieter. Und schließlich ist die Netzwerkökonomie von Industriestandards ein weiterer Grund für die Herausgabe freier Software: nur wenn eine signifikante Anzahl von Benutzern den Acrobat Reader von Adobe einsetzt, werden ihre Geschäftspartner diese Software ebenfalls installieren; mit jedem weiteren Nutzer dieser Software wächst ihre Interoperabilität überproportional. Der gleiche Mechanismus gilt natürlich auch für Betriebssysteme, Mobilkommunikation, Standards für den Dokumentenaustausch, Java, Datenbanken oder den kostenlosen Starwriter 5.0 von StarDivision.

Der Shareware- und Freeware-Markt für Software spielte hier eine Vorreiterrolle. Heute kann ein Neuanbieter seinen zukünftigen Erfolg nur durch freies Verfügbarmachen seines Produktes für Frühnutzer (early adoptors) sichern. Die Folge ist, daß es zukünftig zwei extreme Varianten der Produktneuentwicklung geben wird: Entweder das „Linux-Modell“ oder das „Brechstangen-Modell“.

- Im ersten Fall wird bei minimalen Kosten (im wesentlichen Freizeit) eine kleine Komponente als Baustein komplexerer Software entwickelt. Dabei fallen weder Marketing- noch Verwaltungskosten an. Der Entwickler kann seine Komponente im Überblick behalten, so daß der übliche Koordinations-Overhead eines Software-Projekts entfällt. Die Zielsetzung ist meist klar definiert (Linux-Treiber, Buchhaltungssoftware, GUI-Komponente).
- Dem zweiten Modell liegt ein kostspieliger Produktionsplan zugrunde: eine Produktentwicklung, die möglicherweise nicht viel komplexer als die Shareware-Buchhaltung ist, erfordert mindestens einige Millionen Euro an Investitionsaufwand, damit Kosten der Entwicklung, Verwaltung und Vermarktung gedeckt werden können. Das Unternehmen kann sich nicht darauf verlassen, daß die Entwickler „bei der Stange“ bleiben, daher ist ein erheblicher Mehraufwand für die Entwicklungsleitung zu kalkulieren. Die somit erlangte Berechenbarkeit hat jedoch einen hohen Preis.

In beiden Fällen ist der kommerzielle Erfolg nicht garantiert, jedoch ist der potentielle Verlust im zweiten Fall erheblich höher. Weiter oben wurden die Vollkasko- und die Free-Ökonomie hinsichtlich des Sicherheitsrisikos unterschieden. In ähnlicher Weise lassen sich hinsichtlich der unternehmerischen Herangehensweise die Linux- und die Brechstangen-Ökonomie unterscheiden – mit dem Unterschied, daß hier nicht die Transaktionskosten, sondern die Investitionskosten das wesentliche Unterscheidungskriterium ausmachen. Auch hier stehen im Prinzip beide Welten für ein Softwareprojekt offen: in der Linux-Variante wird begrenztes Kapital eingesetzt (eben Freizeit), um eventuell als begabter Entwickler Aufmerksamkeit zu erlangen, während in der zweiten zunächst ein Investor zu begeistern und im Anschluß eine komplexere Entwicklungsorganisation in Bewegung zu setzen ist.

Die Rolle des Electronic Commerce liegt wiederum in der Schaffung einer Marktinfrastruktur, die beide Varianten für alle Beteiligten zuläßt. In der Tat liegt diese Situation heute in vielen Fällen vor. Manager von Risikokapital-Fonds von Konzernen oder Privatinvestoren haben immer ein offenes Ohr für Produktideen und sind zahlreich im Internet vertreten (XXX, XXX, XXX). Ebenso sind Shareware-Entwickler mit ihren Produkten auf eigenen „Marktplätzen“ zu finden (XXX, XXX, XXX).

→ XXX Einsatz von Idea Future als Free-Economy-Mechanismus???

4.2.7 Aufmerksamkeitsökonomie

Vertreter der Aufmerksamkeitsökonomie, wie z.B. Goldhaber [Gold98] oder Franck [Fran98], sehen in der Aufmerksamkeit ein dem Geld ähnliches Gut, welches im Austausch gegen Dienstleistungen, Geld oder Aufmerksamkeit selbst „gehandelt“ werden kann. Aufmerksamkeit wird zum knappen Gut, wenn der Alltag des Menschen bereits durch die gegebene Informationsflut ausgefüllt ist. Zudem löst eine auf Aufmerksamkeit basierende Ökonomie die Geldökonomie ab, wenn eine materiell vollständige Absicherung bei den Teilnehmern des „Aufmerksamkeitsmarktes“ gegeben ist. In diesem Augenblick treten Bedürfnisse in den Vordergrund, die durch Geld nicht unmittelbar befriedigt werden können (z.B. Präsenz in den Massenmedien). Das Internet erzeugt dabei eine Hebelwirkung, die über die Emanzipierung des Einzelunternehmers einer weitaus größeren Zahl von Teilnehmern hilft, internationale Aufmerksamkeit zu erhalten. Goldhaber schreibt hierzu:

„Das wirkliche Versprechen des Webs, des Netzes und ähnlicher Dinge ist, auch wenn es niemals gänzlich eingelöst werden kann, daß sie einem helfen, das immer stärker werdende Bedürfnis nach Aufmerksamkeit zu befriedigen. Um Aufmerksamkeit zu erhalten, muß man das aussenden, was man technisch mit Information gleichsetzen kann. Genauso muß Information, um irgendeinen Wert zu besitzen, Aufmerksamkeit erlangen. Daher ist die Informationstechnologie auch eine Aufmerksamkeitstechnologie oder, um es anders zu sagen, wird eine Informationsübertragung nur dann erfolgreich sein, wenn es auch eine Aufmerksamkeitsübertragung in der entgegengesetzten Richtung gibt.“

Aufmerksamkeit fließt somit zwischen den Teilnehmern der Internet-Ökonomie. Sie kann untereinander vermittelt werden, z.B. mit Hilfe von Banner-Tauschprogrammen, bei denen nicht im Wettbewerb stehende Teilnehmer jeweils Werbebanner der anderen auf ihrer Homepage einblenden, sie kann erworben und auf Konten der „Aufmerksamen“ gebucht werden und sie kann schließlich wieder in materielle Güter gewandelt werden – wenn z.B. der Linux-Entwickler sie durch einen „fetten Auftrag“ versilbert.

Goldhaber geht jedoch sogar soweit, daß er die Aufmerksamkeitsökonomie vollständig von der materiellen Ökonomie abkoppelt, sie sogar als inkompatibel empfindet. Dies zeigt sich am brennendsten beim geistigen Eigentum an immateriellen Gütern (Musik, Literatur). Dadurch, daß die Nutzung des Werkes durch die Hürde des Lizenzvertrags begrenzt wird, steht hier die Aufmerksamkeit im Widerspruch zum materiellen Gewinn. Geistiges Eigentum heißt, daß niemand aufmerksam sein darf, der dafür kein Geld bezahlt. Selbst wenn die Menschen das Geld hätten, wird ihnen dieses Problem, vor allem im Internet, zu schwierig sein, und sie werden ihre Aufmerksamkeit auf das richten, was weniger kompliziert und frei verfügbar ist.

Für ein Buch wie dieses bedeutet es beispielsweise, daß es frei im Web verfügbar gemacht werden sollte – es ist leichter mit Suchmaschinen zu finden und lenkt die Aufmerksamkeit von weitaus mehr potentiellen Lesern auf Autor und Betreiber des Web-Servers als die reine Buchproduktion. Das „Kauf-Buch“ wird dann in gebundener Form im wesentlichen wegen seines höheren Lesekomforts bezahlt. Warten wir mal ab, ob eine entsprechende Einigung mit dem Verlag erreicht werden kann ;-)

Die Aufmerksamkeitsökonomie kann damit als Erweiterung der „Free Economy“ aufgefaßt werden: Bei der letzteren tritt Aufmerksamkeit nur als Vehikel zur späteren Erlangung materiellen Gewinns auf. Erstere sieht im Extremfall sogar eine Entkopplung von der traditionellen Ökonomie vor. Dies ist heute am ehesten im Bereich der wissenschaftlichen Publikation gegeben, die außer der Buchung auf einem Aufmerksamkeitskonto zunächst keinen materiellen Rückfluß einfordert. Als „Gewinnfunktion“ dient hier der *S(cience) C(itation) I(ndex)*, ein Zitationsindex, der die Anzahl von Referenzen wissenschaftlicher Literatur sammelt und damit als Meßplatte für Aufmerksamkeit dient. Im Gegenzug zur Aufmerksamkeit liefert der Autor Information, deren Qualität durch die Anzahl an Zitaten ausgedrückt wird.

Auch wenn es die Ökonomie der Aufmerksamkeit bereits solange gibt wie Werbung betrieben wird, im Internet kann sie jedoch auf Mikroeinheiten heruntergebrochen werden. In diesem Bereich denke man an Effekte wie Personalisierung und Atomisierung von Werbeinformation. Folglich sind Informationen und Werkzeuge, die zum richtigen Zeitpunkt bei den richtigen Personen Aufmerksamkeit wecken oder erhalten, heiß begehrt. Zu diesen Werkzeugen zählen beispielsweise Kundenprofile und Software, die zur Verfeinerung dieser Profile eingesetzt

werden kann.

4.2.8 Disintermediation: Vom Händler zum Makler

Anfang dieses Jahrhunderts war die Ford Motors Company quasi ein "Staat im Staate", d.h. jede der erforderlichen Ressourcen und Lieferanten waren Bestandteil der Konzernorganisation: Kautschuk wurde in Kolumbien angebaut, durch Ford-eigene Transportorganisationen zum Zentralwerk geliefert und dort zur Produktion der Ford-Autoreifen eingesetzt, die wiederum nur für Ford-Automobile verwendet wurden. Diese Wertschöpfungskette war hinsichtlich Aufbau und Ablauf zentral und tief organisiert. Im Laufe der Jahrzehnte wandelte sich der organisatorische Zusammenhang dieser Kette in Richtung immer kürzerer Glieder, die jeweils anderen Unternehmen zugeordnet waren. Ursache waren zum einen die Standardisierung von Produkten, Prozeduren und Daten, zum anderen jedoch auch die Fähigkeit spezialisierter Unternehmen, schneller auf Marktveränderungen zu reagieren.

Heute nun ist diese Standardisierung soweit fortgeschritten, daß aus organisatorischer Sicht ein integriertes und gleichzeitig hochflexibles Gebilde aus Funktionseinheiten Güter und Dienstleistungen erstellt. Es wird damit quasi zur Nebensache, welcher Organisation die jeweiligen Funktionseinheiten ökonomisch und juristisch zugeordnet sind.

Gleichzeitig besteht jedoch gerade wegen der Standardisierung und Flexibilität auch die Möglichkeit, jederzeit das externe Angebot für die Funktion eines Gliedes gegen ein internes - als "Make or Buy"-Entscheidung - zu prüfen, so daß weniger die sachliche Zugehörigkeit einer Funktionseinheit zum Unternehmen als Entscheidungsgrundlage für die "Buy"-Option gilt als vielmehr ihre Rentabilität.

Aus dieser Situation des "Stöpselns und Konfigurierens" heraus ist die zunehmend wichtigere organisatorische Anforderung an die Informationstechnologie im Unternehmen erkennbar. Diese schlägt sich in der Nutzung so banaler Dienste wie e-Mail nieder und erstreckt sich über die Standardisierung des Elektronischen Datenaustauschs (EDI) bis hin zur Integration hochflexibler Softwarekomponenten als sog. Business Objects.

...

Neben dieser Flexibilisierung von Wertschöpfungsketten hin zur Marktöffnung ist durch den Einfluß von Internet-Standards auch eine Veränderung ihrer Zusammensetzung erkennbar: Während heute noch der Vertrieb physischer und ideeller Güter über eine klassische Kette aus Hersteller, Exporteur, Importeur, Großmarkt und Einzelhandel zum Kunden gelangt, beginnen in einer Vielzahl Branchen immer mehr Glieder wegzubrechen:

In Bereich der Versicherungen erobern Direktversicherungen einen zunehmenden Marktanteil.

Apotheken werden bisher von Grossisten beliefert, deren besonderer Service es ist, mehrmals täglich "on-demand" auch kleine Arzneimittelmengen an jede einzelne Apotheke zu liefern. Zur diesem Zweck besitzen diese ein proprietäres Terminal, mit dem über Modem-Verbindungen Bestellungen veranlaßt werden. Grossisten wiederum bestellen ihrerseits bei Pharmaherstellern, wie z.B. Bayer, Schering oder Glaxo. Für einen solchen Hersteller stellt sich heute durchaus die Frage, ob nicht aufgrund der effizienten Internet-Logistik das Bestellwesen und die damit verbundene Warenwirtschaft internalisiert und für die Auslieferung mit Kurierdiensten kooperiert werden sollte. Dabei entfällt die Funktion des Wiederverkäufers, welche durch die des Lieferdienstes ersetzt wird. Letzterer spielt jedoch nur eine sekundäre Rolle in der Wertschöpfungskette.

Noch drastischer wird die Situation bei immateriellen Gütern. Greifen wir hier einmal das Musikgeschäft heraus:

Eine Band nimmt einige Songs auf CD auf und bietet ihr Oeuvre einem Musikverlag zur Publikation an. Dieser schließt mit den Künstlern einen Vertrag zur Vermarktung des Produktes und preist es seinerseits wiederum Produzenten, Plattenunternehmen etc. an. Evtl. kooperiert dieser Musikverlag mit ausländischen Partnern, da dies einer landesgerechten Vermarktung sowie hinsichtlich der unterschiedlichen Verwertungsgesellschaften (GEMA etc.) vorteilhaft ist. Schließlich wird ein geringer Bestandteil der bereitgestellten Inhalte vom Schallplattenunternehmen produziert, gepreßt, vermarktet und über Handelsketten vertrieben. Je nach Definition erstreckt sich dabei die Wertschöpfungskette über 5-8 Stufen. Dabei könnte heute alles so einfach sein: Die Band nimmt ihr Stück auf, generiert eine Mpeg-3 Audio-Datei und bietet sie für DM 1,- über ihren Webserver an. Sie verdient dabei mehr als im klassischen Modell. Der Endkunde bezahlt weniger und muß nicht auch noch diverse uninteressante Stücke bezahlen, die aus Gründen der Vollständigkeit auf die CD produziert wurden. Die Wertschöpfungskette besteht nur noch aus 2 Stufen - Hersteller und Endkunde. Alle weiteren Beteiligten sind Sekundärdienste, wie Telekom-Provider, Internet Service Provider, Banken (für die Bezahlung) und evtl. Marketing-Unternehmen zur Promotion des Produkts.

XXX...

An den Beispielen ist zu erkennen, in welchem Ausmaß sich der Weg vom Hersteller zum Endkunden von der Handelskette wegbewegt hin zu einer beliebigen Anzahl Maklern.

Dieser Prozeß wird aufgrund der Verkürzung der Kette um ihre mittleren Glieder Disintermediation genannt. Dabei kommt dem Makler (engl. Broker) eine wachsende Bedeutung zu: Er registriert und kategorisiert Angebote und Anfragen von Marktteilnehmern, er vermittelt aktiv Kooperationspartner, indem diesen die Adressen der Gegenparteien übermittelt werden und er läßt sich auf verschiedene Weise nutzen, um anhand komplexer Spezifikationen ganze Konsortien zur gemeinsamen Herstellung oder Abnahme eines Produktes zu formieren (vgl. Abschnitt XXX).

...

4.2.9 Commoditization

Commoditization beschreibt die Wandlung vormals komplexer Güter, die nur von wenigen benutzt werden (konnten) zu allgemein verfügbaren und einfach anwendbaren. Beispiele sind Flugreservierungssysteme, Internet-Werkzeuge, PCs, etc. Am Anfang ihrer Entwicklung waren diese Produkte komplex, sie besaßen eine unhandliche Benutzerschnittstelle und nur Experten konnten sie bedienen. Entsprechend waren dies keine Produkte, die für den Massenmarkt entwickelt wurden. Aufgrund ihrer begrenzten Stückzahl wurden sie (oder ihre Nutzung) zu einem hohen Preis angeboten.

Als „Commodities“ stehen diese Produkte heute jedem zur Verfügung, ihre Komplexität ist minimal – zumindest die Spezifikation der grundlegenden Produkteigenschaften. Während der Prozess der Commoditization früher Jahre bis Jahrzehnte erforderte, besteht heute die Möglichkeit, aufgrund der schnellen Verbreitung von Information und der Verwendung vorgefertigter-Standardkomponenten eine Idee zum Gebrauchsgut binnen weniger Monate zu entwickeln. Man denke z.B. an den Umgang mit MP3-Audio-Clips.

4.2.10 Virtual Communities

In der physischen Welt bilden sich Gruppen durch langfristige Bindungen wie z.B. innerhalb der Familie, der Schulklasse, dem eigenen Stadtteil oder am Arbeitsplatz. Innerhalb dieser Gruppen werden auch Gedanken zu Themen ausgetauscht, die nicht unmittelbar mit dem Gruppenziel in Verbindung stehen. Folglich kennen sich die Mitglieder entsprechend lang und gut. Durch die Zufälligkeit ihrer Beziehung haben die Mitglieder der Gruppe unterschiedlichste Neigungen, Erfahrungen und Interessen – Unterschiede werden dabei abstrahiert. Bei virtuellen Communities ist dies grundlegend anders. Hier trifft sich eine beliebige Anzahl Mitglieder ad hoc und meist zu einem vordefinierten Thema. Bei einer virtuellen Community werden Mitglieder durch ihr gemeinsames Interesse zusammengehalten. Ähnlich dem Konzept der „One-Product-Company“ kann eine virtuelle Community als „One-Interest-Community“ verstanden werden.

Beispiele für virtual Communities sind Online-Fangemeinden, Online-Skatspieler, Kunden eines Softwareherstellers die sich als Interessengruppe formieren, Interessengruppen zu einem technischen oder gesellschaftlichen Thema oder auch die klassischen Communities wie Stadtteile, Schulklassen oder Projektgruppen im Unternehmen, die „virtuell“ effizienter kommunizieren können.

Der Vorteil einer virtual Community liegt in ihrer Effizienz: In einer Mailliste zum Thema „Standardisation of Digital Signatures for XML“ treffen sich internationale Experten, es sind keine Mühen zur Findung oder Ausbildung des Gesprächspartners erforderlich und die Kosten der Community sind – verglichen mit regelmäßigen Konferenzreisen – drastisch günstiger.

Systeme, die virtual Communities unterstützen, können daher als effiziente Marktplätze für Ideen definiert werden: die Zutrittsbarrieren sind minimal, der „Handel“ kostet lediglich Zeit, und durch ihre Internationalität kann eine noch so spezialisierte Gruppe durchaus einige hundert Mitglieder umfassen.

Durch die niedrigen „Investitions- und Transaktionskosten“ in virtual Communities sind Lebensdauer, Signifikanz und Sichtbarkeit einer Community beliebig gering. Sie stehen damit im Wettbewerb um Aufmerksamkeit ihrer Mitglieder. Wird eine AOL-Chatgruppe langweilig, verlassen Neuzugänge sie binnen weniger Sekunden. Das gleiche ist aber auch bei professionellen Gruppen der Fall, wenn vielleicht die Hürde des „subscribe“ und „unsubscribe“ etwas höher hängt ist.

Heute ist eine spiralförmige Entwicklung zu beobachten, die zur einer weiteren Explosion virtueller Communities in den nächsten Jahren führen dürfte:

1. Immer mehr Menschen nutzen das Internet
2. Damit entstehen immer weiter spezialisierte Interessenausprägungen und der Bedarf nach Transparenz
3. Softwareentwickler stellen Werkzeuge her, mit denen das Einrichten und Verwalten virtueller Communities drastisch vereinfacht wird. Häufig überläßt man einfach der Öffentlichkeit, das System selbst zu verwalten und profitiert nur noch von der Banner-Werbung.
4. Diese Senkung der Eintrittsbarriere bewegt viele weitere Teilnehmer, in eine Community einzutreten, und damit wird das Internet für zusätzliche Nutzer attraktiv.

Stand der Entwicklung ist die natürliche Integration von „Electronic Commerce“ im Sinne des Online-Verkaufs über Shopping-Malls mit der Verwaltung von Online-Communities. Der Online-Kauf kann sich beispielsweise als zusätzliche Aktivität in der Community ergeben. Gleichzeitig dient die Community zur Produktinformation, Beratung und dem Support nach dem Kauf. Dadurch ist ein weitaus engerer Kontakt zu nachfragern und Käufern möglich, der im nächsten Schritt zur Verfeinerung des Produktes genutzt werden kann. Für Online-Anbieter ist ein unverfälschter Feedback-Kanal eines der Hauptinteressen.

4.2.11 Coopetition

Coopetition – die Kooperation zwischen Wettbewerbern – hat verschiedene Motive: Eines ist die Zwangssituation, aufgrund der eigenen begrenzten Ressourcen einen Auftrag zusammen mit der Konkurrenz abwickeln zu müssen, ein anderes die Spezialisierung der Kooperationspartner. Auch die Vermeidung von Risiken kann zur Coopetition führen. So kann eine virtuelle Bank alle erforderlichen Funktionen direkt von der Konkurrenz anmieten und damit ein vollständiges Sortiment an Bankdienstleistungen anbieten (Vgl. z..B. die ENBA-Bank im XXX Manager-Magazin, März99). Für die virtuelle Bank lohnt es sich, da sie ihre Fixkosten minimieren kann und die „Zulieferer“ von Dienstleistungen wie Kontoführung oder Wertpapiertransaktionen können Überkapazitäten sinnvoll nutzen.

Es ist allerdings ebenfalls zu berücksichtigen, daß unser heutiges Klassifikationssystem für Branchen und Geschäftsbereiche zu grobkörnig geworden ist: Unternehmen wie Intershop und Brokat sind auf den ersten Blick Softwareunternehmen – also Konkurrenten – die bei der Entwicklung von Shop-Software kooperieren. Schaut man genauer hin, ist zu erkennen, daß beide extrem spezialisiert sind: Intershop auf das Mall-System und Brokat auf die Payment-Funktion. Damit sind sie auch keine unmittelbaren Konkurrenten mehr. Setzt man eine entsprechende Spezialisierung hin zum Ein-Produkt-Unternehmen voraus, wird die Kooperation sogar zwingend erforderlich.

4.2.12 Geistiges Eigentum

Die klassische Ökonomie hat über Jahrhunderte Mechanismen herausgebildet, die es dem Eigentümer geistiger Rechten erlaubt, diese wahrzunehmen. National und international werden Register und Verzeichnisse für Patente, Copyrights und Warenzeichen verwaltet. Ideen werden dadurch zu handelbaren „Softgoods“. Der dahinterstehende gesetzliche Rahmen versucht, den Interessen aller Beteiligten gerecht zu werden: Innovatoren, Autoren und Urheber, die eine formale Handhabbarkeit ihres geistigen Gutes benötigen, fordern eine strengere Kontrolle über die Verwendung dieser Resultate. Alle anderen fordern hingegen eine Lockerung, damit der kommerzielle Nutzen der Innovation rasch allen zur Verfügung steht.

Der Einfluß des Internet begünstigt erst einmal beide Parteien: Der Innovator kann seine Resultate einer hohen Anzahl Interessenten schnell zur Verfügung stellen, jedoch ist die Kontrolle über die korrekte Behandlung schwach, da Ideen in Form international zugreifbarer, digitaler Güter noch schneller kopiert werden können. MP3 dient wieder einmal als typisches Beispiel. In allen Industriestaaten wird daher die Behandlung geistigen Eigentums extrem kontrovers diskutiert. Während die „Traditionalisten“ die Gültigkeit der bestehenden Gesetzgebung im Internet fordern (was sicherlich juristisch schnell belegt werden kann), vertreten einige andere die Gegenposition, daß in der Internet-Ökonomie andere Mechanismen vorherrschen, die eine Verlagerung des Nutzens bewirken. Das sich über das Internet eine weitaus größere Anzahl Nutzer direkt kontaktieren läßt, kann die Auswirkung einer freien Herausgabe von Werken, Wissen oder ähnlicher Werte über die Steigerung der Aufmerksamkeit zur kommerziellen Ausnutzung im „Folgegeschäft“ führen.

Die zweite Position läßt sich dem Konzept der Free-Economy zuordnen, während sich die erste der Vollkasko-

Ökonomie subsumieren läßt. Entsprechend aufwändig wäre im zweiten Fall auch die Infrastruktur: Die Sammlung und Verwaltung von Rechten müßte durch entsprechende Online-Datenbanken erfolgen, die in Form von TrustCentern Zertifikate verwalten, die den Besitz einer Lizenz oder die Urheberschaft belegen. Der Handel solcher Rechte würde ebenfalls immer eine Datenbank-Aktualisierung bei solchen Trusted-Third-Parties erfordern.

Eine prominente Vertreterin des Free-Economy-Ansatzes ist Esther Dyson. Ihr Argumentation ist etwa folgendermaßen: Da die Aufmerksamkeit das eigentlich knappe Gut seitens des Käufers ist, besteht das höchste Ziel eines Anbieters, Autors etc. in der Gewinnung einiger Minuten dieser knappen Ressource. Da Inhalte die Aufmerksamkeit von Individuen binden, schreibt dieser Handel eine ganz neue Rollenverteilung vor: Der Anbieter ist der Konsument oder der potentielle Nutzer des geistigen Gutes. Der Nachfrager nach eben dieser Aufmerksamkeit setzt das geistige Gut als Zahlungsmittel ein, um den Interessent für seine Aufmerksamkeit zu entlohnen. Dieses Geschäftsmodell ist beispielsweise beim Privatfernsehen etabliert, wo der Zuschauer für das Ansehen der Werbespots mit interessanten Inhalten bezahlt wird. Ester Dyson unterscheidet dabei folgende grundlegende Sgeschäftsmodelle, zwischen denen ein fließender Übergang besteht [Dyso97]:

- Abonnements. Hierbei wird ein kostenloser „Teaser“ lediglich zum Wecken des Interesses genutzt, eine Dienstleistung zu abonnieren. Dabei liegt der ökonomische Nutzen in der Höherwertigkeit der Produkte, die nur zahlenden Mitgliedern zur Verfügung stehen. „Höherwertig“ bedeutet z.B. vollständig (Musikstücke), qualitativ besser (höhere Bitmap-Auflösung) oder aktueller (5 Minuten Verzögerung der Börseninformation, während 10 Minuten bereits kostenlos sind).
- Auftritte. Bereitstellung des MP3-Clips auf dem Internet. Der Live-Auftritt der Band kostet allerdings Eintritt. Gleiches gilt auch für den Ausbildungsbereich.
- Intellektuelle Dienstleistungen. Z.B. Unternehmensberatungen, die Fallbeispiele aus der Vergangenheit veröffentlichen. Diese Herausgabe von Know-How motiviert Interessenten, ihnen einen Auftrag zu vergeben.
- Elektronische intellektuelle Dienstleistungen. Ein Übersetzer könnte einen automatischen Übersetzungsdienst betreiben. Zur Steigerung der Qualität wurde er die Korrektur solcher Rohfassung vollständig über das Internet anbieten können. Gleiches gilt für Software-Updates und Ferninstallationen.
- Mitgliedschaften. Ähnlich dem Abonnement-Modell bietet die Mitgliedschaft, eine Möglichkeit innerhalb einer geschlossenen Benutzergruppe qualitativ hochwertige Informationen auszutauschen, ohne Gefahr, daß diese kurzfristig an die Öffentlichkeit gelangt. Im gegensatz zum Abonnement ist die Mitgliedschaft ein symmetrisches Modell, bei dem jeder aufgefordert ist, Inhalte zu liefern.
- Konferenzen mit persönlich anwesenden Teilnehmern. Während das Auslifern von Inhalten per Download kaum kosten verursacht, ist die Inanspruchnahme eines Experten kostspielig. Ein Online-Beratungsgespräch im Sinne eines Call-Centers oder ein multimediales Online-Seminar ist daher ein typisches Folgegeschäft, nachdem Inhalte kostenlos zur Verfügung gestellt wurden.
- Kundendienste. Die Wartung einer frei herausgegebenen Software ist die Grundlage aller Shareware. Hier erhält man die Version n+1 häufig nur gegen Bezahlung.
- Koppelprodukte. Auch hierbei werden Koppelprodukte aufgeteilt in freie und preisbehaftete. Dabei zieht das elektronische Portemonnaie von Brokat oder CyberCash die Installation eines zu bezahlenden Payment-Servers auf der Händlerseite nach sich.
- Werbung. Yahoo lebt fast ausschließlich von Banner-Werbung. Dabei sind die angebotenen Dienstleistungen kostenlos um die Anzahl der potentiellen Kunden zu maximieren. Das gleiche Geschäftsmodell gilt für fast alle Online-Services die über eine hinreichend große Community verfügen. Die große der Community läßt sich dabei anhand präziser Kennzahlen messen.
- Sponsoren. Hierbei erfolgt die Produktion von Inhalten aufgrund der Alimentation durch Dritte. Dies könnte etwa der Staat sein, der Universitätsprofessoren, Filmproduktionen oder öffentliche Konzerte sponsert. Ein Inhalteanbieter könnte aber auch als Sponsor seiner selbst auftreten, indem er einem Web-Server über sein Hobby-Thema aufsetzt. Er sponsert diesen Inhalt mit seiner entgangenen Arbeitszeit.

Bei jedem dieser Ansätze dient die Herausgabe freier Inhalte ein Schlüsselement, welches gleichzeitig den Übergang von der Free-Economy zur klassischen motiviert. In der letzteren werden schließlich die Rechte an grobkörnigen Gütern wie Seminarveranstaltungen oder Koppelprodukten in traditioneller Weise gehandelt. Es erfolgt damit ein stetiger Wechsel zwischen den Markmodell, ohne daß man es als Teilnehmer bemerkt.

Auch für diesen Bereich gilt damit die gleiche Anforderung wie bei der Wahl der Ökonomie: Dem einzelnen Teilnehmer muß transparent sein, mit welchem Marktmechanismen er bei welcher Ökonomie konfrontiert ist, damit eine bewußte Entscheidung für das Agieren getroffen werden kann. Jeder muß selbst entscheiden, ob er

sein Buch ohne Anspruch auf Copyright im Internet zur Verfügung stellt oder ob es auf dem traditionellen, aber beschwerlicheren Wege veröffentlicht werden soll.

4.2.13 Individualisierung

„The Market of You“ titelt die „Encyclopedia of the New Economy“ diesen Effekt im WIRED-Magazin [XXX]. Angesichts einer zunehmenden Vereinfachung der Produktspezifikation (siehe: „Commoditization“) stehen Anbieter unter dem Druck, Alleinstellungsmerkmale herauszubilden, die Kaufanreize beim Kunden bewirken. Ein Weg ist hier bei der Individualisierung. In der physischen Welt wird dies bei Produkten wie Jeans, Einbaurückensitzen oder Autos praktiziert. Hier konnten die Kosten der Individualisierung so stark reduziert werden, daß sie gegenüber der Massenware preislich kaum wahrnehmbar sind.

Im Internet besteht nun die Möglichkeit, mit einer einmaligen Investition in ein Profil-Managementsystem Kunden ein individuelles Angebot zu unterbreiten. Dies rechnet insbesondere bei Soft-Goods, die bereits in feinkörniger Struktur vorliegen und deren Klassifikation automatisierbar ist. Folglich sind Nachrichtenagenturen die ersten gewesen, die individualisierte Presseinformationen einer Kunden-Community anbieten konnten, ohne daß die Individualisierung zusätzliche Betriebskosten verursacht.

Über das Internet können damit Inhalte preiswert, persönlich und automatisiert angeboten werden. Allerdings sind der Individualisierung Grenzen gesetzt, denn nur wer sich selbst klassifizieren kann, kann auch Produkte wählen. Ein Service, der es erlaubt CD-Roms mit Musikstücken zu brennen nützt wenig, wenn man nicht weiß, welche Produkte man auswählen soll. Die klassische Ökonomie lebt davon, bekannten und gewünschtes mit unbekanntem und vielleicht auch unerwünschtem zu koppeln. Nur selten kauft man eine Zeitschrift nur wegen eines einzelnen Artikels – noch seltener liebt man nur diesen Artikel, wenn man sie gekauft hat. Es sind die anderen 95% des Inhalts, die das Bedürfnis nach Information befriedigen. Eine Individualisierung für die Massen kann folglich zu einer Herausbildung von monothematischen Interessen und damit einer reduzierten Kommunikationsfähigkeit über die eigenen virtuelle Community hinaus führen.

4.2.14 Mikrofinanzierung oder $10 * \text{kleines Risiko} < 1 * \text{großes Risiko}$

Größe bedeutet Verwaltung und Verwaltungsaufwand hemmt Entwicklung und Innovation. Aus diesem Grunde verstehen sich Großunternehmen wie die Deutschen Telekom oder Oracle heute weniger als Baumeister denn als Gärtner. Der Gärtner verschafft seinen Start-up-Pflänzchen ein Klima, in denen sie sich optimal entwickeln können. Zunächst werden alle Unternehmen mit der Gießkanne aufgezogen und erfahren die gleiche Pflege und Betreuung. Wenn erkennbar ist, daß sich einige als lukrative Prachtexemplare entwickeln, wird die Pflege verstärkt. Andere werden aus Treibhaus entfernt, um neuen Unternehmen Platz zu bieten. Eine wichtige Stufe in der Entwicklung der Prachtexemplare ist der Börsengang – hierbei besteht die Möglichkeit, durch einen Emissionskurs, der erheblich über dem Nominalwert einer Aktie liegt, nicht nur die Investition in das eine Unternehmen auszugleichen, sondern auch jene in die erfolglosen.

Die Hebelwirkung einer erfolgreichen Produktentwicklung ist in der Internet-Ökonomie so hoch, daß Raum zur Kompensation der jeweils hohen Teilrisiken eines Investment-Portfolios bleibt. Es erfordert jedoch beträchtliches Fingerspitzengefühl und Grintkenntnis der technologischen Basis eines Geschäftsplans, um vorab bereits Perlen unter den potentiellen Start-Ups zu erkennen.

Ein hochinteressantes Beispiel, wie der Ansatz der Mikrofinanzierung nationalen Volkswirtschaften und Kulturen umwälzen kann, hat die Grameen Bank in Bangladesch bewiesen. Anstelle die üblichen Großprojekte wie Staudämme, Kraftwerke und Fabriken zu fördern, bei denen das Risiko möglicherweise sogar moderat ist, hat besagte Bank an den Graswurzeln der Gesellschaft angesetzt und Mikrokredite von bis zu 50 Dollar oder weniger an potentielle Unternehmer vergeben. Das Schlüsselement dieser Maßnahme war eine besondere gesellschaftliche Kenntnis: Frauen stellen in der Gesellschaft Bangladeschs die Hauptträger der körperlichen Arbeitsleistung dar. Zudem besteht bei ihnen eine besondere Kultur der Aufrichtigkeit und Leistungswilligkeit. Durch die Förderung insbesondere von Frauen als Mikrounternehmerinnen konnte somit eine gesellschaftliche Veränderung bewirkt werden, die nicht nur einen emanzipatorischen Effekte hat, sondern dadurch auch eine radikale ökonomische Besserstellung bewirkte.

Die Intelligenz der Mikrofinanzierung liegt folglich in der Kombination aus kulturellem, technischen und ökonomischen Know-How und der Streuung der Finanzierungsmaßnahmen auf eine Vielzahl von Unternehmen.

4.2.15 Elektronische Märkte

Vor über zehn Jahren hat Thomas Malone analysiert, daß angesichts „Elektronischer Hierarchien und elektronischer Märkte“ [XXX] tendenziell zu erwarten ist, daß das Prinzip des Marktes als externe Koordination von Angebot und Nachfrage jenes der Organisation, die die Produktion zentral organisiert durch die Entwicklung des Internet stärker begünstigt wird. Dies ist bereits heute der Fall: in hohem Maße besteht heute für einen Innovator die Möglichkeit, seine Idee eigenständig am Markt durchzusetzen, indem das Internet als ebenes Pflaster zur Unterstützung sämtlicher Transaktionsphasen dient. Die Transparenz ist dabei so hoch, daß ein Anbieter wie www.ibm.com genauso schnell kontaktiert werden kann wie z.B. www.ponton-hamburg.de.

Insbesondere im Bereich der intangiblen Güter (Information, Musik, Beratung) entstehen Monat für Monat neue Marktsegmente. Dabei drängt sich mehr und mehr die Frage auf, wie die Idee des elektronischen Marktes effizient unterstützt werden kann. Welche Komponenten sind erforderlich, um den Marktteilnehmern ein freies agieren als Anbieter oder Nachfrager zu ermöglichen? Eine zu komplexe Architektur – zu der wir als Ingenieure häufig neigen – kann schnell kontraproduktiv wirken. Das Paradebeispiel ist hier die TINA-Architektur der Telekom-Gesellschaften: Während diese sich in der ersten Hälfte der 90er Jahre noch mehrere hundert Millionen schwere Gedanken über ein Konzept zur Erfassung aller relevanten Bausteile und Mechanismen zur Unterstützung einer internationalen multimedialen Telekom-Diensteplattform machten, emergiert gleichzeitig das WWW aus den Ideen einer handvoll Köpfe. Die Hebelwirkung des Internet war wahrscheinlich noch nie so drastisch erkennbar wie bei diesen beiden Entwicklungen hin zu einer Plattform. Während sich der TINA-Koloß noch heute im Beta-Stadium der Standardisierung befindet, können wir über das Internet Informationen austauschen, handel treiben und demnächst auch multimedial kommunizieren.

Zurück zum Thema des elektronischen Marktes: So wie Märkte in der physischen Welt emergieren und dabei neue Formen des Handels etablieren können, so erfolgt dies auch im Internet. Der Unterschied liegt jedoch wieder in der Entwicklungsgeschwindigkeit. Beim elektronischen Markt lohnt es sich häufig nicht, in die Standardisierung einer Komponente zu investieren, da ihre Funktionalität bereits nach einem Jahr – also dem Minimum der zur Standardisierung erforderlichen Zeit – wieder erweitert oder grundlegend modifiziert wird.

Einem idealen elektronischen Marktplatz muß folglich das technologische Kunststück gelingen, jene Komponenten die zwingend für seinen Betrieb erforderlich sind, zu standardisieren und andere, die sporadisch oder in kleineren Communities genutzt werden oder die noch nicht den nötigen Reifegrad erlangt haben, den Anwendern zur Eigenentwicklung offenzulassen. Schließlich sollte eine elektronische Marktplattform das Standardisieren selbst standardisieren, so daß eine Anwendungskomponente, wenn sie denn allgemein als Standard akzeptiert wird, in die Plattform integriert werden kann.

Diesem Thema ist mein Buch „Elektronische Dienstmärkte“ gewidmet, das aus einer eher theoretisch-technischen Perspektive Phänomene des elektronischen Marktes behandelt [XXX Merz99].

4.2.16 Das Gesetz des einzigen Preises

Die Transparenz auf dem elektronischen Markt führt im Extremfall zur vollständigen Information aller Beteiligten über den Preis, den ein Anbieter aufgrund seiner Kostenstruktur fordern kann. Bereits heute kann ein Importeur von PC-Komponenten vom Preis eines Komplett-PC ablesen welche Komponenten zu welchem Preis verwendet wurden und in welcher Höhe die Gewinnspanne liegt. Ein Abweichen von diesem Wert nach oben ist sofort für versierte Kunden erkennbar und damit für den Anbieter nicht realisierbar. Gleiches gilt für Hypothekenkredite, Aktienkurse an unterschiedlichen Börsenplätzen, Flug- oder Autopreise etc.

Der Ökonom spricht hier von Symmetrie bzgl. der Produktinformation, d.h., es gibt keine verborgenen Informationen des Anbieters, dies es ihm erlauben einen höheren Preis zu verlangen. Dies sind natürlich schlechte Nachrichten für Händler und Arbitrageure, die von Asymmetrien und Intransparenzen profitieren. In Verbindung mit der „Commoditization“ sowie der Standardisierung von Produktbeschreibungen sind auch Computer zunehmend in der Lage, Preisunterschiede zu erkennen. Solche automatischen Preisagenten bieten bereits für das Anschauen eines Werbebanners einen Vergleichsservice.

Das Refugium der Arbitrageure wird der konsequenterweise der Bereich bleiben, in dem einseitiges Wissen aufgrund komplexer Produktbeschreibungen erforderlich ist – also alle Dienstleistungen, die eher in Projektform erbracht werden oder Produkte, bei denen aufgrund ihres geringen Marktvolumens nur eine verzerrte Marktpreisbildung erfolgen kann.

4.3 Die Rolle des Staates

Der Staat ist der wichtigste Mitspieler auf dem nationalen Markt. In Deutschland beträgt die Staatsquote beispielsweise 48 Prozent, d.h., je nach Berechnungsform tritt er in dieser Größenordnung als Nachfrager oder Anbieter auf. Neben dieser Rolle als Teilnehmer ist er jedoch auch Organisator des Marktes. Natürlich nicht im Sinne einer Planwirtschaft (obwohl die hohe Staatsquote dies in Deutschland fast vermuten läßt), sondern als die Instanz, welche die Spielregeln für die Marktteilnehmer definiert.

Als Gesetzgeber gewährt sich der Staat das Recht, bestimmte Strukturen und Prozesse marktwirtschaftlichen Koordination zu durch Gesetze zu regulieren, so daß der Erhalt von Werten gewährleistet bleibt, die über die der ökonomischen Effizienz gestellt werden. Zu diesem Zweck ist es Aufgabe des Staates, Konsumenten und ihre Privatsphäre zu schützen, die intellektuellen und kommerziellen Rechte der Marktteilnehmer zu schützen und die Gesellschaft vor politischen oder ökonomischen Verzerrungen zu bewahren. Gleichzeitig tritt der Staat als Sponsor von Dienstleistungen und Gütern auf, die für einzelne Marktteilnehmer zu kostspielig wären oder nicht in unabhängiger, neutraler Form erbracht werden könnten (Ausbildung, Gesundheitswesen, Straßennetz, kulturelle Unterhaltung etc.).

Eines der wichtigsten Güter, die ein Staat produzieren kann ist jedoch Vertrauen. Nur bei genügend hohem Vertrauen in das Gemeinwesen, kann eine Handelstransaktion ohne permanente Absicherung gegen Betrug und ähnliche Risiken durchgeführt werden. Eine Arbeitslosenversicherung wäre nichts wert, wenn man dem Staat nicht zutrauen würde, einen auch noch in zwanzig Jahren gegen das Risiko des Arbeitsplatzverlustes zu versichern. Gleiches gilt für die Rechtsprechung und die innere Sicherheit. Der Staat kann auch als Qualitätsanker auftreten, z.B., wenn er einen Mindestanteil an Wortbeiträgen für Radiosender fordert oder selbst mit privaten Anbietern in Konkurrenz tritt.

Ein Staat existiert jedoch nicht isoliert sondern selbst im Wettbewerb mit anderen Staaten. Auch ohne Internet besteht beispielsweise seit Jahrzehnten der Wettbewerb zwischen den Regionen Nordamerika, Europa und Asien. Die beteiligten Staaten stehen unter dem Druck, ihre Marktplattform so effizient wie möglich zu gestalten, um einen ökonomischen Vorteil gegenüber dem Wettbewerb zu erzielen. Dies gilt u.a. für die Bereiche Bildung, Zölle, Bauverordnungen und vor allem für die Steuergesetzgebung.

In der Vor-Internet-Zeit war es im globalen Maßstab lediglich das Kapital, das als Wirtschaftsfaktor für Investitionen oder Anlagen mobil eingesetzt werden konnte. In der Internet-Ökonomie sind vor allem die Faktoren Arbeit und Information hinzugekommen, die zusammen mit der nochmals beschleunigten Mobilität des Kapitals international angeboten und nachgefragt werden.

Wenn nun über das Internet Dienstleistungen gehandelt werden können, die in Irland einhundert Euro und in Deutschland 200 kosten würden (wie z.B. das Übersetzen eines Artikels vom deutschen ins englische), so kann sich dies im Internet zu einer virtuellen Migration von Arbeitskräften führen, die nicht der Regulation des Zielandes unterworfen sind. Folglich gerät die Regierung des „teuren“ Staates unter Druck, die Kostenstruktur der eigenen Marktanbieter besserzustellen, was international zu weiterem Wettbewerb führt. Dies muß natürlich nicht in den Zustand des ruinösen Wettbewerbs entarten, da kulturelle und ökonomische Faktoren wie Bildung und (Rechts-)Sicherheit eine wichtige Rolle bei der Wahl des Geschäftspartners spielen.

Staaten werden somit selbst zu einer Ware, deren Erfolg am Markt für Standorte bewertet wird. Als Makler tritt dabei beispielsweise die Weltbank auf, die entscheidet, ob ein Staat besser als andere eine nachhaltige Entwicklung, die Reduzierung der Armut oder eine Anpassung an den Wandel erzieht hat.

Globalen Märkte sind keineswegs Systeme, die nach objektiv feststellbaren Mechanismen funktionieren. Die subjektive Bewertung eines Staates gleich eher einer Wette, die auf seinen Erfolg abgeschlossen wird. Aus der Aggregation aller Wetten ergibt sich jedoch ein repräsentatives Bild, das die Einschätzung der Weltöffentlichkeit widerspiegelt. Dabei spielt die Glaubwürdigkeit eine zentrale Rolle, die selbst drastische Unterschiede im Preisniveau rechtfertigt.

Ein Bericht der Weltbank („Rethinking the State“) aus dem Jahre 1997 analysiert die [Weltbank97] Rolle des Staates angesichts einer zunehmenden Globalisierung, die vor allem durch die Internet-Ökonomie gefördert wird. Er kommt zu dem Schluß, daß "Märkte und Regierungen komplementär" seien. Die Beschaffenheit des Staates und seiner institutionellen ist ein entscheidender Faktor für die Wettbewerbsfähigkeit seines Standortes. Die Glaubwürdigkeit der Regierung, gemessen in der Vorhersagbarkeit ihrer Entscheidungen und ihrer Politik sowie in der Konsistenz ihrer Umsetzung, kann für private Investoren ebenso wichtig sein wie deren Inhalt.

Folglich ist die Rolle des Staates als Qualitäts- und Stabilitätsanker nicht nur national sondern auch international zu verstehen. Dem Weltbank-Bericht zufolge liegt diese Rolle in einer Partnerschaft mit Wirtschaft und Gesellschaft:

Florian Rötzer kommentiert den Bericht folgendermaßen [Telepolis 1997, [http://www.tp.de/special/eco/Rethinking the State.htm](http://www.tp.de/special/eco/Rethinking%20the%20State.htm)]:

„Als Grundlage gilt daher, von manchen als ‘Terror der Ökonomie’ gebrandmarkt, schlechterdings die Wirtschaft, der sich die Politik anzupassen habe, aber man hält deutlich fest, daß die (National)Staaten weiterhin eine zentrale Rolle spielen und daß ihre Stabilität entscheidend für die wirtschaftliche Entwicklung ist. Im Dienste der globalen Ökonomie erscheint der Staat als entscheidender Sicherheitsfaktor, der Recht und Ordnung aufrecht erhält und extreme Ungleichheiten abmildert, die den globalen Markt gefährden, vor allem aber ihn selbst zu einem unattraktiven Standort werden lassen könnten. Explizit wird festgestellt, daß der Staat - und damit die territorial gebundenen demokratischen Repräsentanten eines Volkes - kein Souverän mehr ist, daß es keine Volkswirtschaften mehr gibt, was eben auch heißt, daß die Menschen keine Souveräne im Sinne des Ideals ‘Wir sind der Staat’ mehr sind, sondern nur noch als ‘Partner, Katalysatoren und Fördernde’ eines schicksalhaften Prozesses fungieren. Wer nicht mitmacht, geht unter: das ist die Botschaft in nuce.“

Man mag über Electronic Commerce denken, wie man will, das Prinzip des Wettbewerbs abstrahiert von organisatorischen Strukturen und hebt das Individuum über die Unternehmung und diese über den Staat. Angesicht einer solchen Entwicklung ist nur schwer abzuschätzen, welche sozialen und ökonomischen Auswirkungen politische Entscheidungen haben und wie stark sich die höhere Umlaufgeschwindigkeit der Wirtschaft auf eine höhere Umlaufgeschwindigkeit des Staates auswirkt.

Nachdem die Rolle des Staates bisher nur abstrakt angesichts einer sich wandelnden Weltwirtschaft skizziert werden konnte, sollen im folgenden einige wenige Beispiele zeigen, in welcher Weise der Staat mit speziellen Randeffekten des Electronic Commerce konfrontiert ist.

4.3.1 Notenbanken in einer bargeldlosen Wirtschaft

Die Aufgabe der Notenbank liegt in der Geldpolitik, d.h. insbesondere in der Steuerung der Geldmenge sowie in der Festlegung des Zinsniveaus. Die Geldmenge wird üblicherweise im Bargeldumlauf sowie in Form von Girokonten und kurzfristigen Sichteinlagen gemessen. „Eigentümer“ des im Umlauf befindlichen Bargeldes bleibt die Notenbank, wir sind lediglich Besitzer der Scheine und Münzen mit dem Recht auf Umtausch, z.B. in eine andere Währung.

Da die Notenbank das im Umlauf befindliche Bargeld nicht verzinst, andererseits jedoch diesen Betrag zins- oder ertragbringend verleihen kann, erzielt sie in der Regel einen Gewinn – die sog. *Seignorage*. Einen Teil dieses Gewinnes schüttet sie an den Staat aus. Wenn nun (wie in Abschnitt XXX beschrieben) für die Zukunft zu erwarten ist, daß anstelle des Bargeldes zunehmend elektronische Zahlungsverfahren eingesetzt werden, hat dies zwei Effekte: erstens wird die Nachfrage nach Bargeld reduziert und zweitens verliert die Notenbank an Einfluß bei der Steuerung des Bargeldumlaufs.

Durch die Reduktion der Bargeldnachfrage wird sich nun auch das Volumen an Bargeld reduzieren, d.h., der Notenbank-Gewinn wird vermindert. Bei verringerter Bargeldnachfrage bietet sich für die Konsumenten normalerweise als Alternative die Anlage in verzinslicher Form an, damit sollte eigentlich zu erwarten sein, daß sich der Gewinn von der Notenbank zum Konsumenten hin verschiebt. Dies ist jedoch nicht der Fall, da durch die Herausgabe von Zahlungssystemen wie z.B. der Geldkarte, die Verzinsung des Kartenbetrages nicht für den Konsumenten erfolgt (für ihn ist die Karte nur eine Verlängerung des Girokontos), sondern für den Kartenherausgeber (die Bank), die von der zinslosen Anlage des Girokontos profitiert.

Wenn nun dieser Bargeldumlauf ein Volumen annimmt das nicht mehr durch die Geldpolitik der Notenbank steuerbar ist, verliert der Staat ein wichtiges volkswirtschaftliches Steuerinstrument, über das heute wirtschaftspolitische Zielsetzungen wie z.B. die Inflation innerhalb gewisser Grenzen durchgesetzt werden können.

Die Realität wird sich nicht so drastisch entwickeln wie diese Perspektive vermuten läßt, da zum einen der Gesetzgeber die Möglichkeit hat, durch regulatorische Maßnahmen eventuelle negative Entwicklungen zu verhindern und zweitens der Einsatz elektronischen Geldes nur allmählich und in geringem Maße erfolgen wird.

Die Europäische Zentralbank forderte allerdings im August 1998 in ihrem "Report on Electronic Money" eine Regulierung des elektronischen Geldes, da man zu der Überzeugung gekommen ist, daß elektronisches Geld in Zukunft für die Geldpolitik relevant werden kann. Dabei wurden sechs Mindestanforderungen gestellt:

eine angemessene Überwachung der Herausgeber elektronischen Geldes,

- klare Regelungen der rechtlichen Beziehungen,

- Gewährleistung technischer Sicherheit,
- Schutz gegen kriminellen Mißbrauch,
- Informationspflichten gegenüber der Zentralbank,
- eins zu eins Umtauschbarkeit von elektronischem Geld in Zentralbankgeld und
- die Option, elektronisches Geld mit einer Mindestreserve zu belegen.

Darüber hinaus werden die Interoperabilität der Systeme und der Schutz gegen das Risiko des Geldverlusts (durch Verfahren wie sie zur Einlagensicherung heute üblich sind) angestrebt.

Die EZB hat sich grundsätzlich das Recht vorbehalten, selbst elektronisches Geld zu emittieren

4.3.2 Zoll und Steuern

1998 veröffentlichte das Information Society Project Office (ISPO) der EU-Kommission einen Bericht, in dem vorgeschlagen wurde, für alle Daten, die über private und öffentliche Netze fließen, eine "Bitsteuer" zu erheben. In der Industrie und bei Privatkunden stieß dieser Vorschlag natürlich auf entschiedene Ablehnung. Heute hat sich diese Diskussion abgekühlt, sicherlich auch weil für den Staat bzw. die EU-Kommission deutlich wurde, daß eine derartige Maßnahme auch bisher unbesteuerter Telefonate treffen würde. Damit würde diese Beschneidung weit über den Electronic Commerce hinaus auch die Kommunikation von Privatpersonen treffen und somit der heute allgemein gewünschten Deregulierung im Telekommunikationsbereich entgegenwirken.

Nach XXX (Telepolis, „Die bargeldlose Gesellschaft“) arbeiten die Regierungen aufgrund der Ablehnung der Bitsteuer andere Pläne aus, um neue Besteuerungsmöglichkeiten zu erschließen: Die in Europa verfolgte Alternative liegt in einer indirekten Bitsteuer im Energiesektor. In einem 1998 verabschiedeten Beschluß [XXX] schlug die Europäische Kommission eine Regelung vor, die ein allgemeines Steuersystem auf Energie in der EU einführt. Es ist offensichtlich, daß die Europäische Kommission dabei Telearbeit mit berücksichtigt hat, denn "der Beschluß verlangt auch den Übergang der Steuerlast von der Arbeit zu anderen Sektoren wie dem der Energie."

Abgesehen von der Bitsteuer wird über das automatische Abführen der Mehrwertsteuer nachgedacht, wie 1998 vorgelegte Pläne von Ira Magaziner, der Senior-Beraterin des amerikanischen Präsidenten in Sachen Internet, zeigen [XXX Wall Street Journal 11 Sep 98]. Diesem Vorschlag zufolge sollen Electronic-Commerce-Teilnehmer sog. „Resident Card“ zum Bezahlen benutzen, mit deren Hilfe Händler feststellen könnten, in welchem Land sich ein Kunde befindet und welche Steuer anzuwenden ist. Abgesehen von der Landeskennung würden keine weitere Personendaten an den Händler herausgegeben werden. Mit Hilfe privatwirtschaftlicher Steueragenten würden Verbrauchssteuern gesammelt und an die Steuerbehörde des betreffenden Landes überwiesen werden. Auf diese Weise würden Staaten schneller zu Ihren Steuereinnahmen gelangen.

Es bleibt abzuwarten, ob die Staaten hier teilnehmen und ob die Verteilung des Steueraufkommens zwischen den Staaten in naher Zukunft etabliert werden kann. Auch in der Europäischen Union wird über solche Verfahren nachgedacht.

4.4 Gewinner und Verlierer beim EC

Grundsätzlich kann man sagen, daß in jeder Branche die Chance besteht, sich auf die Gewinnerseite zu schlagen. Es sind eben eher die schnellen und ersten, die Kapital aus der höheren Umlaufgeschwindigkeit des Handels ziehen können. Verlierer sind damit die Riesen, für die bereits der Versionswechsel des Betriebssystems (zugegebenermaßen eines recht komplizierten) als 10-Millionen-Euro-Projekt verbucht werden muß – für derartige Kosten gibt die Gewinnmarge zukünftig kaum mehr Freiraum her.

Gewinner sind aber auch auf Nischenmärkten zu finden. Man nehme die Unterhaltungsindustrie, speziell Computerspiele: In dieser Boom-Branche wandelt sich das Produkt "Spiel" zunehmend vom Meisterstück eines Kunsthandwerkers zum Resultat eines komplexen Produktionsprozesses, der mit Hollywood-Filmproduktionen

keinen Vergleich scheuen braucht. Hier entstehen neue "Zuliefermärkte", etwa für die Produktion von Avataren, für Filmeinspielungen, Spiele-Engines, die ein effizientes Movement-Management für Actionspiele nach dem Baukastenprinzip bieten usw. Mit Sicherheit werden etliche neue Branchen und "Business Cases" entstehen, fraglich ist jedoch, ob diese die "freigesetzten" Heerscharen der Bankangestellten, Versicherungsverkäufer und Verwaltungsangestellten absorbieren können – sowohl quantitativ als auch hinsichtlich ihrer Qualifikation.

Gewinner und Verlierer lassen sich nicht vollständig nach Berufsgruppen trennen, vielmehr kann man erwarten, daß das Wirtschaftsleben eher den Charakter einer Lotterie im Sinne der „Hollywood-Ökonomie“ annimmt – allerdings mit erheblich höheren Einflußmöglichkeiten der Mitspieler: Wer eine innovative Idee mit der richtigen Finanzierung und geeigneten Mitarbeitern kombiniert, hat durchaus die Chance, einen Lottogewinn zu produzieren. Dabei spielt die Kombination dieser Faktoren eine wesentliche Rolle: Fünf "harmonisierende Schumpeters", die den richtigen Investor überzeugen konnten, haben heute eine erheblich größere Chance auf einen Lottogewinn als der Konzern, welcher seinen selten kreativen Direktoren und Bereichsleitern ein Vielfaches an Budget zuteilt. Natürlich hat der Konzern seine Lebensberechtigung – z.B. als Garant für die Lieferung von Ersatzteilen auch noch nach Jahrzehnten. Die Innovation erfolgt jedoch immer mehr außerhalb seiner Grenzen. So ist es ein übliches Ziel des Silicon-Valley-Start-Ups, von Microsoft absorbiert zu werden, wie es 1997 gleich drei Video-Streaming gleichzeitig "widerfahren" ist: Sowohl (XXX Stimmen die Namen???) V-Extreme, Real als auch XXX wurden als potentielle Konkurrenz vom Markt weg-internalisiert. Für die Gründer hat sich diese Transaktion sicherlich gelohnt, genauso wie für den Konzern.

Wie bereits angedeutet, verlagert sich der Innovationsprozeß weg von der geplanten Produktpalette hin zur Hollywood-Produktion: Viele Filme enden als Flop, einige sind rentabel und wenige werden zur Goldgrube. Dieses Verhältnis gilt natürlich auch für die Entwicklungsabteilung des Konzerns, nur wird es zunehmend für kleine Unternehmen an Bedeutung gewinnen. Es wird eher spekulativ gearbeitet, das Risiko für den Investor steigt damit, jedoch auch die Aussicht auf einen "Blockbuster" der Hi-Tech-Industrie. In Deutschland sind da beispielsweise die Unternehmen Intershop und Brokat zu nennen (siehe auch weiter unten im Abschnitt XXX), die heute (März 1999) immer noch in der Verlustzone liegen und dennoch für ihre Investoren eine Goldgrube waren. Beide Unternehmen wurden Anfang der Neunziger zu Beginn der Internet-Euphorie gegründet. Beide besetzten mit Online-Shops und Internet-Banking-Software eine Wachstumsnische, die schließlich nach wenigen Jahren zum "Going-Public" am Neuen Markt führte. Für den Investor ist dieser Augenblick der seltene Moment der Bescherung, nachdem er sich jahrelang gefragt hatte, ob denn nicht Kommunalobligationen doch die bessere Anlageform gewesen sein könnten. Jetzt nämlich kann er nach der Steigerung des Kurswertes der Intershop- und Brokat-AG seine Ernte einfahren und sich neuen Start-Ups widmen. Die Geburtshilfe eines neuen "Konzerns" wurde erfolgreich geleistet.

Wenn vielleicht nicht immer in dieser zugespitzten Form, so könnten sich doch diese Symbiosen aus Finanzierung und Intelligenz in Zukunft zum Standardmodell eines liberalisierten Marktsystems entwickeln. "Electronic Commerce" bewirkt in diesem Zusammenhang eine stärkere Polarisierung: die Schnellen werden immer schneller und die Langsamen bleiben auf der Strecke. Die Kleinen können bei hohem Risiko kurzfristige Vorteile besser nutzen, während die Großen, bei niedrigerer Rentabilität, jedoch dank Diversifizierung abgemildertem Risiko als langfristiger Garant der Ersatzteillieferung zur Verfügung stehen. (XXX Ausdruck!). Die sozialen Auswirkungen sind dabei kaum absehbar; ihnen ist der Abschnitt XXX gewidmet.

Wenn sich also auf nationaler Ebene kaum Verlierer identifizieren lassen, dann vielleicht auf internationaler? Man kann feststellen, daß sich die US-Wirtschaft im Hinblick auf ihre Industrieproduktion zwischen Januar 1998 und Januar 1999 mit 1,9% Zuwachs besser entwickelt hat als Deutschland (+0,8%) bzw. die EU (+1,5%).

XXX bessere Zahlen finden!!!

4.5 Soziale Auswirkungen

Soziale Auswirkungen des EC sind zum heutigen Zeitpunkt nur schwer quantifizierbar – weder hinsichtlich der zeitlichen Verlaufs zukünftiger Entwicklungen, noch hinsichtlich ihrer konkreten Effekte. In folgenden sollen daher nur exemplarische Bereiche erwähnt werden.

4.5.1 Computerkriminalität

Die wesentlichen Bedrohungen im Bereich des EC lassen sich unter den folgenden Begriffen subsumieren:

- Kreditkartenbetrug
- Erpressung
- Geldwäsche
- Diebstahl
- Raubrittertum
- Etikettenschwindel
- Spionage und andere klassische Angriffsszenarien

Die ersten drei sind im Bereich elektronischer Zahlungsverfahren anzusiedeln. Diese werden als Werkzeug krimineller Aktivitäten eingesetzt. Diebstahl hat nur bedingt mit EC zu tun, da er auch ohne EC erfolgen kann, ohne daß Parteien Handel treiben. Andersverhält es sich beim Diebstahl elektronischen Geldes. Unter Raubrittertum ist das kurzfristige Öffnen eines Online-Shops zu verstehen, der nur dem Zweck dient, Zahlungen einzuziehen, ohne die Ware zu liefern. Nach einer Woche wird der Shop wieder geschlossen und die Konten des Händlers aufgelöst. Etikettenschwindel steht für die Vortäuschung einer Markenzugehörigkeit oder eines nicht gegebenen Qualitätsniveaus.

Laut [BöRi98] nimmt beim Bargeld der Anteil von Zahlungen mit Falschgeld einen verschwindend geringen Anteil ein: Bei einem Kaufhauskonzern mit Milliardenumsätzen fallen Falschgeldzahlungen in Höhe von wenigen tausend DM an. Hier liegt die Betrugsrate bei Kreditkarten bereits um den Faktor 10 höher. Expertenaussagen zufolge konnten die Kosten des Kreditkartenbetrugs in den letzten Jahren allerdings von 0,5 Prozent auf ca. 0,1 Prozent gesenkt werden. Sogar im sog. MoTo-Bereich (Mail-Order, Telephone-Order), bei dem weder physische Nähe noch das Leisten einer Unterschrift erforderlich ist, erwarten die Experten keine wesentlichen Bedrohungen im Zusammenhang mit dem Electronic Commerce. Eine Veränderung dieser Daten aufgrund der häufigeren Verwendung von Kreditkarten im Internet kann noch nicht festgestellt werden.

Trotzdem ist zu berücksichtigen, daß ein erfolgreicher Angriff im Bereich der elektronischen Zahlungsverfahren erheblich gravierender sein kann, als herkömmliche Geldwäsche oder Betrugsszenarien: Für den Fälscher bieten sich ideale „Economies of Scale“. Kопierte oder mit gestohlenen Schlüsseln signierte Geldeinheiten lassen sich nahezu beliebig herstellen. Außerdem sind gefälschte elektronische Münzen nicht erkennbar. Oder wenn beispielsweise ein Online-Buchhandel, dessen Jahresumsatz im Bereich einiger hundert Millionen liegt, einfach für zwei Wochen seinen Umsatz einzieht und auf ein Nummernkonto überweist. Nun ist die Internet-Öffentlichkeit beispielsweise bei Amazon.Com hinreichend sensibilisiert – das Unternehmen steht jeden Tag im Rampenlicht, aber ein unbekanntes Online-Unternehmen, das eine Woche lang in Form von Kleinbeträgen 100.000 Euro einzieht, ohne die Ware zu liefern – dies ist durchaus denkbar und in der Praxis bereits vorgekommen:

Vor einigen Jahren inserierte ein deutsches Unternehmen in gängigen Computer-Zeitschriften mit Preisen, die mindestens 10-20 Prozent unter dem üblichen Marktpreis lagen. Hunderte von Bestellern wurden geprellt, als der Unternehmer sich nach wenigen Wochen einschließlich seines „Umsatzes“ absetzte. Letztlich war es der Gemeinschaft aus Verlag, seriösen Anbietern und kritischen Lesern zu verdanken, daß dieser Betrug schnell auffliegen konnte. Das sichergestellt Geld reichte jedoch nicht zur Schadenserstattung allen Besteller. Es ist fraglich, ob eine solche Situation sich im Internet ähnlich abspielen könnte: Entweder kann es leichter fallen, solche Straftaten zu begehen, da andere sich aufgrund der höheren Anonymität nicht um den Übeltäter kümmern oder das Internet hilft, Nachrichten über solche Unternehmen schneller zu verbreiten. Hier wäre ein Schwarze-Listen-Service, der regelmäßig von Browsern kontaktiert wird, sicherlich sehr hilfreich.

Folglich gilt auch für den Herausgeber elektronischen Geldes, daß eine Sicherheits- und Vertrauensinfrastruktur aufzubauen ist, die hilft, alle Beteiligten vor einem „E-Geld-GAU“ zu schützen. Hierbei kann es beispielsweise gefährlich sein, elektronisches Geld mit einem einzigen Signierschlüssel zu „prägen“. Wenn jemand diesen einen Schlüssel stiehlt, besteht im schlimmsten Fall die Möglichkeit, eine beliebige Geldmenge zu fälschen.

Erpressung ist theoretisch möglich, wenn im Internet ein vollständiges Äquivalent zum Bargeld existierte, daß anonyme Bezahlungen ohne Verzögerung auf Workstations an jedem Ende der Welt erlaubt. Durch eine technische Limitierung des Maximalbetrages auf wenige hundert Euro läßt sich dieser Gefahr jedoch schnell begegnen. Außerdem ist ein System wie Ecash darauf angewiesen, daß der Zahlungsempfänger sein elektronisches Geld über einen zentralen Server verifizieren läßt. Da dies nicht-anonym erfolgt, kann er mit Hilfe von Fangschaltungen und aufgrund des hohen Geldbetrags ermittelt werden.

Geldwäsche ist ein weiteres Delikt, das prinzipiell über das Internet ausgeübt werden könnte. Zur Geldwäsche ist jedoch immer Bargeld erforderlich, um ein Aufspüren von Kontenbewegungen zu vermeiden. Eine häufige Erscheinungsform ist dabei das Fingieren von Verkäufen über Ladengeschäfte. Dies ist natürlich auch auf der Ebene von Micropayments denkbar, jedoch würde es hier schwerfallen, das zur Geldwäsche erforderlich Volu-

men unerkannt zu erzielen. Außerdem besteht auch bei elektronischem Geld immer die Möglichkeit, Bewegungsprofile zu erstellen, so daß größere Geldbewegungen ermittelt werden können. Letztlich bietet die Limitierung von Transaktionsvolumina auch bei der Geldwäsche eine einfache Handhabe, um die Attraktivität des Mediums zu senken.

4.5.2 Mobilität der Märkte

Wenn denn den neuen, kleinen, schnellen, jungen Start-Ups der Markt der Zukunft gehört, was bedeutet dies für die Lebensdauer dieser Unternehmen? Netscape war auch mal jung und klein, genauso wie Microsoft. Heute existiert nur noch Microsoft. Wie "alt" darf ein Unternehmen also maximal werden, bevor es sich regenerieren muß? Kann man sich ein Unternehmen zukünftig als Reptil vorstellen, welches zwar wachsen kann, aber dabei (und dafür!) regelmäßig einen Teil seines Körpers abstreifen muß?

Wie sieht es dabei mit einem Land wie Deutschland aus, in dem der Altersdurchschnitt der Bevölkerung bei XXX Jahren liegt, während in unmittelbarer Nachbarschaft mit einem Durchschnitt von XXX Jahren eine gut ausgebildete, junge und angriffslustige Generation antritt? *Mobilität* definiert der Volkswirt hinsichtlich unterschiedlichster Wirtschaftsfaktoren: Mobilität des Faktors "Arbeit" bedeutet: "Ubi bene – ibi patria", man folgt dem besten Gehaltsangebot – und wenn dies in Frankfurt, London oder San Francisco liegt. Über Mobilität des Kapitals lesen wir täglich in der Zeitung: Start-Up-Unternehmen werden schnell fallengelassen, wenn sich am Kapitalmarkt rentablere Investitionsmöglichkeiten ergeben. Gleiches gilt für den supranationalen Wettbewerb um Kapital. Investiert wird, wo die Rendite am höchsten ist. Dies gilt vor allem in der virtuellen Weltwirtschaft, bei der der Tante-Emma-Laden am anderen Ende des Globus eingerichtet werden kann (wegen des günstigen Investitionsklimas) und doch nur ein, zwei Mausklicks nah bleibt.

Mobilität im weiteren Sinne bedeutet auch die der Geschäftsbeziehungen: In wenigen Jahren werden wir nicht nur für Telefonverbindungen Least-Cost-Router einsetzen, sondern auch für alle anderen Resultate der Commoditization: Lebensmittel, Autos, Reisen, Hypothekenkredite, Personal, CDs. Werden sich Geschäftsbeziehungen durch wachsende Promiskuität und Beliebigkeit auszeichnen? Wird es Alternativen geben zum heutigen Modell des "Vertrauen durch langfristige Beziehungen" – etwa durch Vertrauensnetzwerke oder ein perfektioniertes Ranking-Verfahren (siehe Abschnitt XXX), das es erlaubt, die mangelnde gemeinsame Erfahrung durch die Nutzung von Ranking-Diensten als vertrauenswürdigen Dritten zu erkaufen. Vielleicht wird man eines Tages jedoch auch feststellen, daß langfristige Beziehungen doch von höherem Wert sind als die unmittelbar meßbaren Vorteile des Least-Cost-Routing. Nicht immer bedeutet "Mehr Markt" gleichzeitig auch mehr Qualität - dies hängt ganz wesentlich von den regulatorischen Randbedingungen des Gesetzgebers ab. Als in Großbritannien beispielsweise der Eisenbahnbetrieb privatisiert wurde, führte dies zu einer erheblichen Qualitätseinbuße, nicht, weil die privaten Betreiber nicht reinvestiert hatten, sondern vor allem weil sie Tickets zum ursprünglichen, niedrigen Preis der staatlichen Bahn anbieten mußten. Diese war jedoch stark subventioniert.

Eine für Soziologen interessante Frage ist sicherlich, in welchem Maße sich die "ökonomische Promiskuität" auf das soziale Leben auswirkt. Diese Auswirkung kann sowohl steigernd im Sinne einer "Beziehung-On-Demand" sein oder auch kompensatorisch im Sinne einer Sehnsucht nach dem dörflichen Ruhepol einer vertraulichen Gemeinschaft.

5 Electronic Commerce in der Informationstechnologie

5.1 Sicherheit und Vertrauen

Unabhängig von Ecommerce-Anwendungen, empfinden Internet-Nutzer ein besonderes Bedürfnis, sich bei ihrer Kommunikation vor möglichen Angriffen Dritter zu schützen. Speziell im Bereich des Ecommerce gilt dies neben dem Schutz der Privatsphäre vor allem auch zur Sicherung von Werten in Form von Geld oder handelbaren Gütern. Aus diesem Grunde ist die Forderung nach Sicherheit und Vertrauen beim Online-Handel so grundlegend, daß sie bei allen EC-Umgebungen und -produkten bereits einer der untersten Architekturebene behandelt wird. Erst wenn „weiter unten“, ein Mindestmaß an Sicherheit und Vertrauenswürdigkeit erfüllt ist, setzen weitere Funktionen wie Zahlungsmechanismen, Online-Kataloge oder Broker-Systeme architekturell auf.

Während sich Fragen der Sicherheit leicht in einige wenige Anforderungen und dazugehörige technische Mechanismen zerlegen lassen, ist die Schaffung von Vertrauen nicht ohne weiteres allein technisch zu erreichen. Hier ist immer die erfolgreiche Integration technischer und organisatorischer Maßnahmen erforderlich.

Der Begriff der Sicherheit umfaßt im Deutschen nicht nur Fragestellungen, die dem englischen Begriff der „Security“ zu subsumieren sind (Autorisierung, Vertraulichkeit, Authentisierung, Integrität und Nichtabstreitbarkeit), sondern auch solche der Zuverlässigkeit, Robustheit, und Ausfallsicherheit. Im folgenden werden wir uns jedoch auf Fragen der „Security“, beschränken, die alleine bereits bündelnd sein können....

Die Schaffung von Vertrauen zielt auf die Vermeidung oder Abwendung möglicher Schäden der Benutzer durch den Betreiber des Marktes oder Dritte ab. Dabei soll ein Marktteilnehmer so agieren können, als ob er sich in einer vollständig vertrauenswürdigen Umgebung befindet – entweder, indem für ihn technisch nachvollziehbar potentieller Schaden ausgeschlossen wird oder indem ein anderer Teilnehmer im Schadensfall die Haftung trägt. Im Gegensatz zur Sicherheitsinfrastruktur besteht hinsichtlich dieser beiden Anforderungen weder in der internationalen Gemeinde von Geschäftspartnern noch im Internet selbst keine vollständig „wasserdichte“, Infrastruktur. Auch beim traditionellen internationalen Handel kommt es regelmäßig zu Betrugsfällen – auch wenn dieser durch politische, juristische und organisatorische Maßnahmen auf erträglichem Niveau gehalten werden kann. Ähnlich verhält es sich mit „vertrauensvollem Electronic Commerce“, – ein Restrisiko ist wahrscheinlich nie auszuschließen. Doch beginnen wir zunächst mit Fragen der Sicherheit:

5.1.1 Autorisierung

Genau sowenig wie es Personen untersagt ist, ohne weitere Berechtigung Privaträume anderer zu betreten, besteht im Internet wie auch innerhalb einer Organisation das pauschale Recht, auf beliebige Ressourcen zuzugreifen. Da in der einen wie in der anderen Welt der alleinige Hinweis auf diesen Sachverhalt weder zufälliges noch böswilliges Eindringen vermeiden hilft, wurden Barrieren errichtet, die nur berechtigte Personen überwinden können. Zum Überwinden dieser Barrieren muß dem System ein Berechtigungsnachweis vorgelegt werden. Alternativ kann dies auch implizit durch Zugehörigkeit zu einer berechtigten Gruppe erfolgen. Sicherheitshalber wird zumeist der Berechtigungsnachweis vom System selbst verwaltet, so daß die Gefahr, durch Fälschung eine Berechtigung zu erschleichen, von vornherein vermieden werden kann.

Betriebssysteme verwalten daher Listen zur Zugriffskontrolle zu Ressourcen wie Dateien, Verzeichnisse, Kommunikationsports, Geräte oder ausführbarer Software. Zur Optimierung der Verwaltung werden Benutzer des Systems zu Gruppen zusammengefaßt, Rechte auf eine überschaubare Menge beschränkt (z.B.: Lesen, Schreiben, Ausführen) und eine entsprechende Kombination dieser Informationen einer Ressource zugeordnet. Einer Datei kann damit beispielsweise zugeordnet werden, welchem Benutzer und welcher Gruppe (der er angehört) welche Operationen erlaubt sind.

Die Verfahrensregel zur Modifikation dieser Informationen ist wiederum auf der Betriebssystemebene „hard coded“,; nur wer ein Schreibrecht auf die Ressource besitzt, kann auch die Autorisierung ändern. Die Rechte eines Nutzers können mit der Zugehörigkeit zu weiteren Gruppen erweitert werden. Folglich stellt diese Information selbst eine sensible Ressource dar, auf die nur Benutzer-Administratoren Zugriff haben können.

Im Bereich von Betriebssystemen sind Fragen der Autorisierung weitgehend geklärt. Dies liegt nicht zuletzt an der relativ einfachen Handhabbarkeit der Zugriffsrechte, wenn der Verwalter der Ressource und diese selbst

derselben Organisation angehören. Der Netzwerk-Administrator der Firma verwaltet schließlich Zugriff auf Hardware und Software, die innerhalb der Organisation installiert ist. Damit kann eine Überprüfung einer Berechtigung innerhalb der Organisation erfolgen.

Schwieriger ist die Autorisierung verwaltbar, wenn die rechtevegebende Instanz von der Ressource getrennt wird. Dann nämlich muß der Benutzer durch Vorlage eines Zertifikates nachweisen, daß er zur Durchführung einer Handlung berechtigt ist. Als Beispiel sei hier auf die Vorlage einer Vollmacht verwiesen, wenn eine dritte Person durch eine Vertragspartei autorisiert wird, im Namen der letzteren zu unterschreiben. Auf der betreffenden Ressource (dem Vertrag) wird eine Handlung durchgeführt (das Unterschreiben), ohne daß sich Ressource und Vertragspartei innerhalb einer organisatorischen Domäne befinden. Durch das Zertifikat wird statt dessen einem anderen – möglicherweise unbekanntem – Ressourcenverwalter die Berechtigung nachgewiesen. Ein solcher Ressourcenverwalter ist im täglichen Leben beispielsweise ein Notar.

Wir werden die zweite Form der Autorisierung wieder aufgreifen, nachdem weiter unten Mechanismen zur Verwaltung von Zertifikaten erläutert wurden.

5.1.2 Verschlüsselung

Die wohl intuitiv am ehesten mit der Kryptographie verbundene Sicherheitsfunktion ist die Verschlüsselung. Hier wird angenommen, daß zwischen zwei oder mehreren Parteien Daten auszutauschen sind, die zwar vom Empfänger, nicht jedoch von potentiellen Angreifern eingesehen werden können. Folglich ist das Dokument in eine Form zu überführen, aus der ein Angreifer ohne Wissen oder Besitz eines speziellen Schlüssels das Originaldokument wieder rekonstruieren kann.

Secret Key / Public Key

Dieser Schlüssel kann entweder der gleiche sein, der zum Verschlüsseln des Dokumentes verwendet wurde (symmetrische Verfahren) oder ein anderer, der zusammen mit jenem zur Verschlüsselung erzeugt wurde (asymmetrische Verfahren). Im zweiten Fall ist die Verwendung der beiden Schlüssel hinsichtlich der Ver- oder Entschlüsselung nicht vorgeschrieben. Wurde jedoch der eine einmal zur Verschlüsselung eingesetzt, kann die Entschlüsselung nur mit dem anderen erfolgen.

Beim symmetrischen Verfahren kann jeder, der sich den einen Schlüssel kopiert, das Dokument lesen. Somit ist hierbei besonders darauf zu achten, daß dieser auf einem sicherem Weg an den Kommunikationspartner transportiert werden kann – man spricht hierbei von einem „sicheren Kanal“, der konkret Transport und persönliche Ablieferung per Diskette bedeuten kann oder den Transfer durch Verschlüsselung mit einem zweiten, bereits vorher verteilten Schlüssel. Das Problem der Verteilung ist damit jedoch nur verlagert. Symmetrische Verfahren werden daher auch „Private Key“-Verfahren genannt, da der Schlüssel niemals in unberechtigte Hände gelangen darf.

Aus diesem Grunde hat sich im Internet das zweite Verfahren durchgesetzt, bei dem vom generierten Schlüssel-paar einer ausgewählt und fortan als „öffentlicher“, und der andere als „privater“, bezeichnet wird. Der private wird – ähnlich dem symmetrischen Verfahren – ebenfalls nicht herausgegeben, auch nicht an andere Kommunikationspartner! Andererseits sollte hingegen der andere Schlüssel allen anderen bewußt zugänglich gemacht, also *veröffentlicht*, werden. Tauschen nun zwei Kommunikationspartner verschlüsselte Nachrichten aus, so verwenden sie jeweils den öffentlichen Schlüssel des Empfängers zur Verschlüsselung. Dieser kann beispielsweise seiner Homepage oder seinen e-Mails entnommen werden. Leitet dieser nun das Dokument zurück, verwendet er den öffentlichen Schlüssel des ursprünglichen Senders. Da in beiden Fällen nur der Empfänger über den korrespondierenden privaten Schlüssel verfügt, kann niemand anderes das Dokument entschlüsseln. Natürlich wird hierbei angenommen, daß der private Schlüssel niemals in andere Hände als die des Eigentümers gelangt.

Gängige Verfahren

Heute existiert eine Vielzahl symmetrischer und asymmetrischer Verfahren. Dabei finden beide ihre Berechtigung in unterschiedlichen Nischen: symmetrische Verfahren sind in der Regel mit weniger Rechenaufwand durchzuführen, andererseits allerdings auch leichter mit Verfahren der Kryptoanalyse zu brechen. Asymmetrische erfordern erheblich höheren Rechenaufwand – sowohl bei der Generierung als auch bei der Ver- und Entschlüsselung und erst recht beim Brechen der Verschlüsselung. Aus diesem Grunde werden symmetrische und asymmetrische Verfahren häufig kombiniert, um ihre jeweiligen Vorteile zu nutzen: Das asymmetrische dient dabei als

Vehikel für den sicheren Transport eines symmetrischen Schlüssels zum Empfänger. Wurde dieser in der vertrauenswürdigen Umgebung des Empfängers gespeichert, kann er anschließend zur weniger aufwendigen Verschlüsselung eingesetzt werden. Um zu verhindern, daß er binnen kurzer Zeit durch einen Angreifer ermittelt werden kann, sollte er in ausreichend kurzen Abständen gewechselt werden. Üblicherweise sind diese Abstände in der Größenordnung einer Stunde jedoch länger als eine durchschnittliche Sitzung z.B. mit einem Online-Shop.

DES

DES (Data Encryption Standard) ist ein symmetrisches Verschlüsselungsverfahren, das 1975 veröffentlicht wurde und im wesentlichen als Forschungsergebnis von IBM betrachtet werden kann. Auch nach über 20 Jahren kryptoanalytischer Durchleuchtung findet es im Bereich der schwachen Kryptographie heute und in Zukunft seine Einsatzbereiche. DES wurde speziell zur Implementierung in Silizium entwickelt. Eine ausführliche Diskussion des Algorithmus findet sich im Buch von Schneier. Seine hauptsächliche Schwachstelle ist die Schlüssellänge von 56 Bit. Mit einem Brute-Force-Entschlüsselungsversuch sollte es heute möglich sein durch Spezialhardware im Werte von weit weniger als 1 Mio. Dollar einen DSA-Schlüssel in weniger als 30 Min. zu ermitteln.

Als Antwort auf dieses Manko wurde Triple-DES (oder auch DESede) entwickelt, das mit Hilfe von drei DES-Schlüsseln (deren Aneinanderreihung eine Länge von 168 Bit ergibt) den Verschlüsselungsvorgang dreimal durchführt: Einmal unter Verwendung des ersten Schlüssels in die Richtung zum Verschlüsseln, dann mit dem zweiten zurück (also eine "falsche" Entschlüsselung) und schließlich wieder mit dem dritten hin zum zweiten Verschlüsseln.

RSA

RSA ist das bekannteste und eines der nachvollziehbarsten Verschlüsselungsverfahren, das nicht mehr aus der Praxis wegzudenken ist. Es ist benannt nach seinen Entwicklern, Ron Rivest, Adi Shamir und Leonard Adleman. Das Patent für RSA wurde im Jahre 1978 angemeldet und läuft XXX ab.

Im Vergleich zu symmetrischen Verfahren ist die Chance, eine RSA-verschlüsselte Nachricht mit dem gleichen Aufwand zu dechiffrieren, so extrem unwahrscheinlich, daß die US-Sicherheitsbehörde erhebliche Exportrestriktionen für diesen Algorithmus festlegte. Zulässig sind außerhalb der USA nur minimale Schlüssellängen von 40 Bit. Auch wenn diese Restriktionen heute zunehmend gelockert werden und man beispielsweise Finanzinstituten außerhalb der USA die Verwendung gewährt, wird der Algorithmus von der NSA nach wie vor in der Kategorie "Waffe" klassifiziert. Innerhalb der USA werden Schlüssellängen von bis zu 2048 Bit gängig – je nach Sicherheitsbedürfnis.

Das wesentliche Merkmal von RSA ist die Verwendung von Schlüsselpaaren, so daß der Algorithmus im Bereich der Publik-Key-Kryptographie eingesetzt wird. Technisch beruht RSA auf der Schwierigkeit, große Zahlen zu faktorisieren, d.h. eine Ansammlung von Primzahlen zu finden, aus denen sich per Multiplikation die Zahl ergibt. Im folgenden ist zum Nachrechnen der Algorithmus kurz am Beispiel skizziert:

1. Wähle 2 große Primzahlen p und q
2. Berechne $n = p * q$ und $z = (p-1) * (q-1)$
3. Wähle eine Zahl d , die relativ prim ist zu z (d.h. sie besitzt keinen gemeinsamen Faktor)
4. Wähle eine Zahl e (den Chiffrierschlüssel), mit der $e * d = x \mid x \text{ mod } z = 1$
5. Teile die Nachricht in Blöcke, so daß die Länge jeden Blocks $\leq n$
6. Um N zu verschlüsseln, berechne $C = N^e \text{ mod } n$
7. Um C zu entschlüsseln, berechne $N = C^d \text{ mod } n$

Resultat:

- e und n bilden den *öffentlichen Schlüssel*,
- d ist der *private Schlüssel*,
- p und q werden verworfen (und dürfen nicht veröffentlicht werden!)

Dieses Verfahren wird an folgendem trivialem Beispiel nachvollziehbar:

Die zu verschlüsselnde Nachricht lautet 6882326879666683. Dies könnte beispielsweise der Bit-String einer E-

Mail-Nachricht sein.

1. Wir wählen $p = 3$ und $q = 11$
2. Dann ist $n = p \cdot q = 33$, und $z = (p-1)(q-1) = 20$
3. Sei $d = 7$. 7 ist relativ prim zu 20, da kein gemeinsamer Teiler außer 1 besteht.
4. Um e zu finden ist folgende Gleichung nach x aufzulösen:

$$7e = x \pmod{20} = 1$$
 Dabei gilt z.B. für $e = 3$
5. Damit kann ver- und entschlüsselt werden. Wir nehmen eine Blocklänge von 1 Ziffer an, da zwei Ziffern > 33 sind, also: 6,8,8,2 ...
6. Verschlüsselung:

$$C = N^3 \pmod{33} = 18$$
 Der verschlüsselte Nachrichtenblock hat damit den Wert 18.
7. Entschlüsselung:

$$N = C^7 \pmod{33} = 6$$
 Damit wurde die Nachricht im Klartext wiederhergestellt.

Aus diesem einfachen Beispiel läßt sich erahnen, welcher Aufwand erforderlich ist, um die Nachricht N zu entschlüsseln, wenn anstelle von $e=3$, $d=7$ Zahlen in der Größenordnung von bis zu 2048 Bit verwendet werden. Auch die Umkehrung von $n = p \cdot q = 3 \cdot 11$ – d.h. die Primfaktorzerlegung von 33 – ist bei entsprechenden Schlüssellängen nur mit unrealistisch hohem Aufwand erreichbar.

Die Verschlüsselung mit RSA erfordert ebenfalls erheblich höheren Aufwand. Nach Schneier [Schn96] erfordern die schnellsten Hardware-Implementierungen des Jahres 1995 ca. 1 Sekunde zur Verschlüsselung von 1 Megabit. In der Praxis erfordern Softwarelösungen für Sicherheitssysteme ca. 1 Sekunde zur Verschlüsselung kleiner Nachrichten (bis zu 200 Bytes). Dies gilt für einen 300-MHz Pentium-II.

IDEA

IDEA (International Data Encryption Standard) wurde Anfang der 90er in mehreren Schritten entwickelt und verbessert. Es gilt neben RSA als eines der stärksten Verfahren und unterliegt keinen US-Exportbeschränkungen, da es außerhalb der USA entwickelt wurde. Aus diesem Grunde wird es von unterschiedlichen europäischen Anbietern von Kryptosoftware eingesetzt. Die Patentrechte hält die Firma Ascom AG in der Schweiz. Für nicht-kommerzielle Zwecke kann IDEA jedoch kostenlos eingesetzt werden.

IDEA ist ein symmetrisches Verfahren, das mit 128-Bit Schlüssellänge arbeitet. Der Algorithmus ist bei [Schn96] sehr anschaulich beschrieben. IDEA ist ein schnelleres Verfahren als DES, mit einem Pentium-II sollte der Durchsatz bei 300 MHz im Bereich einiger MB/s liegen. Mit Hardware-Unterstützung sind über 50 MB zu erwarten.

Diffie-Hellman

Schließlich wollen wir noch einen Blick auf den Algorithmus von Diffie und Hellman werfen, da dieser heute im Bereich von SSL gerne für den Aufbau einer sicheren Kommunikationsverbindung zwischen Web-Browser und -Server eingesetzt wird. Gerade die Möglichkeit, zwei Kommunikationspartnern einen Sitzungsschlüssel zu vereinbaren zu lassen, ohne daß auf beiden Seiten Vorwissen über gemeinsame Parameter zur Generierung besteht, ist besonders interessant für die Ad-hoc-Kommunikation im Internet. Auch wenn ein Angreifer permanent die Kommunikation abhört, besteht für ihn dabei keine Möglichkeit, an den Wert des Schlüssels zu gelangen. Diffie-Hellman wurde 1976 zum ersten mal veröffentlicht und leitete die Entwicklung der Public-Key-Kryptographie ein. Seit 1997 der Patentschutz aufgehoben wurde, ist der Algorithmus jetzt frei verwendbar. Das Verfahren ist fast trivial:

Beide Kommunikationspartner einigen sich auf zwei Werte, n und g . Diese Werte können frei im Netz vereinbart werden, sie können sogar in einer größeren Gruppe von Benutzern vorab festgelegt sein (z.B. durch die Verwendung des gleichen Software-Tools). Einzige Bedingung: n ist eine Primzahl, zu der g modulo n prim ist. Dann

werden folgende Berechnungen durchgeführt:

1. Partner A wählt eine beliebige, große Zahl x und sendet an Partner B die Zahl X , wobei $X = g^x \bmod n$.
2. Partner B wählt eine beliebige, große Zahl y und sendet an Partner A die Zahl Y , wobei $Y = g^y \bmod n$.
3. A berechnet seinen Schlüssel: $k = Y^x \bmod n$
4. Entsprechend berechnet B seinen Schlüssel $k' = X^y \bmod n$

Für beide Schlüssel gilt: k und k' sind gleich $g^{xy} \bmod n$. Niemand, der die Kommunikation verfolgt, kann die Werte k und k' herausfinden, auch wenn g , n , X und Y bekannt sind.

Beispiel:

Für dieses Beispiel verwenden wir der Nachvollziehbarkeit halber wieder simple Werte. Für n und g werden die Zahlen 7 und 31 gewählt.

1. $X = g^x \bmod n$. Für x wählen wir 5, d.h. $X = 31^5 \bmod 7$, also $X = 5$
2. $Y = g^y \bmod n$. Für y wählen wir 7, d.h. $Y = 31^7 \bmod 7$, also $Y = 3$
3. $k = 3^5 \bmod n = 5$
4. $k' = 5^7 \bmod n = 5$
5. Es gilt: $k = k' = 31^{5 \cdot 7} \bmod 7 = 5$

Die Schlüssel k und k' können nun zur Ver- und Entschlüsselung verwendet werden. Dieser Algorithmus kann sogar auf mehrere Parteien erweitert werden, so daß drei, vier oder allgemein N Parteien ihre X -, Y -, und Z -Werte solange im Kreis weiterleiten und -berechnen, daß am Ende (nach $N-1$ Weitergaben eines jeden Zwischenwertes) allen der gleiche Schlüssel k zur Verfügung steht. Etwas mehr Magie zu diesem Thema ist wiederum bei [Schn96] zu finden.

Export-Problem

Verschlüsselungsverfahren zeigen die Eigenschaft, daß mit zunehmender Schlüssellänge auch der Aufwand zum Ermitteln des privaten Schlüssels drastisch steigt. Folglich können kryptographische Methoden ideal mit der laufend steigenden Rechengeschwindigkeit skalieren. Technologisch sind folglich einem regelmäßigen „Update“ durch Schlüsselverlängerung keine Schranken gesetzt. In der Realität unterliegen kryptographische Methoden jedoch patentrechtlichen Nutzungsbeschränkungen (XXX) und vor allem Einsatzbeschränkung aufgrund ihrer Klassifikation als „Waffe“, seitens der USA. Aus diesem Grunde dürfen außerhalb der USA nur Schlüssellängen von max. XXX (RSA) bzw. XXX(YYY) verwendet werden. Dies stellt in vielerlei Hinsicht eine erhebliche Einschränkung, insbesondere für Electronic-Commerce-Anwendungen dar. Glücklicherweise sind in den letzten Jahren zunehmend Softwaresysteme verfügbar geworden, die auf Verfahren basieren, die außerhalb der USA entwickelt wurden (z.B. IDEA), und damit frei verfügbar gemacht werden konnten. Ferner wird im Jahre XXX der Patentschutz für das RSA-Verfahren ablaufen, so daß nicht zuletzt aus diesem Grund die Exportrestriktionen zunehmend gelockert werden: Finanzinstitute sind heute bereits berechtigt, RSA-Schlüssel der Länge XXX zu verwenden. Für die Zukunft ist zu erwarten, daß dies auch für weitere Unternehmen und schließlich auch Privatpersonen gelten wird.

Verschlüsselung auf Kanalebene / Dokumentenebene

Wichtig zu unterscheiden ist die Frage, ob ein Dokument als Sequenz von Bytes verschlüsselt werden soll oder ein Kanal. Im ersten Fall kann das Dokument in verschlüsselter Form auf der Festplatte abgelegt werden, während im zweiten nur bei der Übertragung im Netz Sicherheit gegenüber Angreifern gewährleistet wird. Verfahren wie z.B. SSL dienen diesem Zweck einer Ende-zu-Ende-Verschlüsselung.

Kombination von starker und schwacher Kryptographie

Die Erläuterung der Verfahren hat gezeigt, daß symmetrische und asymmetrische Verfahren mit unterschiedlichen Vor- und Nachteilen behaftet sind. So kostet RSA sehr viel mehr Rechenzeit sowohl bei der Schlüsselgenerierung als auch beim Gebrauch der Schlüssel. Dieser Nachteil wird mit erheblich höherer Sicherheit gegen Angriffe erkaufte. Allerdings recht häufig für kurze Phasen auch die Verwendung von DES, z.B. bei zeitlich begrenzten WWW-Sitzungen, oder solchen, die der Vereinbarung weiterer Schlüssel anderer Verfahren, z.B. IDEA

dienen. Daher findet in der Praxis üblicherweise ein Mix der Verfahren statt. Internet-Banking-Produkte des Unternehmens Brokat (www.brokat.de) verwenden z.B. SSL für den Aufbau einer schwach gesicherten Verbindung, um auf dieser Basis mit Hilfe von IDEA ein zusätzliches, starkes Verfahren einzubetten. In anderen Bereichen wird RSA verwendet, um einen DAS-Sitzungsschlüssel sicher auszutauschen. Dieser Schlüssel wird dann solange verwendet, wie sichergestellt ist, daß ein Angreifer ihn nicht ermitteln kann (wenige Minuten bis eine Stunde). Innerhalb dieser Zeit kann ein größeres Datenvolumen mit wenig Rechenaufwand verschlüsselt und übertragen werden.

5.1.3 Integrität

Ein Angreifer könnte zwischen anderen Teilnehmern übertragene Daten ändern wollen – z.B. Preise, Termine, Namen oder Kontonummern. Daher ist ein Verfahren erforderlich, welches den Kommunikationspartnern die Möglichkeit gibt festzustellen, ob ihre Daten unversehrt beim Empfänger eingetroffen sind. Zu diesem Zweck werden Hash-Algorithmen eingesetzt:

Hash Algorithmen

Hash-Funktionen dienen dazu, zu einer beliebig großen Datenmenge (ausgedrückt durch einen String von Bytes) einen sog. Hash-Wert zu ermitteln, der folgende Eigenschaften erfüllt:

- Er ist in seiner Länge auf eine vorgegebene Anzahl Bytes festgelegt (üblicherweise weniger als 200 Bytes). Da diese Länge meist sehr viel kürzer ist als die Originaldaten, können mehrere unterschiedliche von ihnen zum gleichen Hash-Wert führen – dies nennt man eine Kollision.
- Man kann nicht vom Hash-Wert wieder auf die Originaldaten schließen (daher auch die Bezeichnung "Einweg-Hash-Funktion").
- Jede, auch noch so minimale, Änderung des Original-Strings führt zu einem radikal unterschiedlichen Hash-Wert.
- Daher ist es äußerst unwahrscheinlich, die Originaldaten so zu verändern (d.h. fälschen), daß wieder der gleiche Hash-Wert erreicht wird.

Hash-Werte werden meist auch "Message Digest" genannt – im Deutschen auch "Fingerabdruck" einer Nachricht. Produkte wie PGP oder andere Kryptobibliotheken verfügen über unterschiedliche Hash-Funktionen, von denen MD5 und SHA die gängigsten sind:

MD5

MD5 wurde 1991 von Ronald Rivest entwickelt. Es ist eine Weiterentwicklung von MD4, einer früheren Version. MD5 produziert 128 Bit lange Hash-Werte. Vor kurzem wurde festgestellt, daß MD5 unter bestimmten Bedingungen nicht sehr kollisionsresistent ist, d.h. mit gewissem Aufwand können alternative Input-Nachrichten ermittelt werden, die den gleichen Hash-Wert liefern.

SHA

Der Secure Hash Algorithm wurde von dem NIST (National Institute of Standards and Technology) der USA in Verbindung mit der NSA (National Security Agency) entwickelt. Wie MD5 ist auch SHA eine Weiterentwicklung von MD4. Die Verbesserungen sind jedoch weitreichender als beim MD5: Hash-Werte haben eine Länge von 160 Bit, was das Risiko einer Kollisionsattacke reduzieren hilft. Es wird empfohlen, wenn möglich SHA als Ablösung des MD5 einzusetzen.

Zur Verifikation der Integrität eines Dokuments ist es erforderlich, den Hash-Wert auf einem sicheren Kanal zum Empfänger zu transportieren. Dies erfolgt üblicherweise unter Zuhilfenahme der oben genannten Verschlüsselungsverfahren, so daß ein Angreifer seinen modifizierten Hash-Wert nicht mit dem vom Empfänger erwarteten Schlüssel chiffrieren kann. Zu diesem Zweck könnte jedes beliebige, genannte Verfahren eingesetzt werden. Eine Besonderheit ist jedoch bei asymmetrischen gegeben: Die Verschlüsselung des Hash-Wertes kann als "Unterschrift" des Senders verwendet werden, wenn dieser dazu seinen privaten Schlüssel einsetzt. Damit sind wir beim Thema der "elektronischen Unterschrift" angekommen:

5.1.4 Authentisierung

Allgemein bedeutet "Authentisierung", nachzuweisen, daß eine Nachricht von dem Sender kommt, von dem sie zu sein vorgibt. Der zu vermeidende Angriffsfall ist also ein bössartiger Dritter, der eine Nachricht an einen Empfänger sendet und sich dabei als ein anderer als er selbst ausgibt. Ein klassisches Beispiel ist die Bestellung von 200 Büchern bei Amazon, um den vorgetäuschten Besteller finanziell zu schädigen. Erforderlich ist also für Amazon die Möglichkeit, die Authentizität dieser Bestellung zu verifizieren. Im normalen Leben würde die Bankangestellte oder Kassiererin im Supermarkt die Unterschrift des Kunden z.B. bei einer Kartenzahlung überprüfen. Im Hochsicherheitstrakt des Verteidigungsministeriums oder eines Kernkraftwerkes werden noch weitaus sicherere (und kostspieligere) *biometrische* Verfahren eingesetzt. Diese Verfahren beruhen auf der Erkennung natürlicher menschlicher Identifikationsmerkmale wie z.B. einem Fingerabdruck oder einem Bild der Netzhaut. Auch die Analyse des Bewegungsablauf eines Stiftes beim Leisten der Unterschrift, z.B. auf einem Eingabetafeln, zählt zu den biometrischen Verfahren.

Solange diese Verfahren jedoch noch nicht allgemein Verwendung gefunden haben, muß auf andere Techniken zurückgegriffen werden. Am bekanntesten waren bisher Magnet- oder Chipkarten zum Nachweis der Authentizität. Auf diesen befindet sich – im primitivsten Fall – ein Code, über den man nur durch Besitz der Karte verfügen kann. Andere Karten, wie z.B. die Kundenkarten der Banken, erfordern zusätzlich die Eingabe eines PIN-Codes, der in Verbindung mit der Karte den Kunden identifiziert. Auch hierbei handelt es sich immer noch um Magnetkarten, die durch einfach herzustellende Geräte ausgelesen oder manipuliert werden können. Nur die weiter unten beschriebenen SmartCards sind in der Lage, aufgrund ihres eigenen Prozessors und einer sicheren Betriebssystemarchitektur solchen Angriffen zu widerstehen.

Insgesamt kann also die Authentizität eines Teilnehmers durch Merkmalsbereiche nachgewiesen werden:

- Durch den *Besitz* eines Gegenstands (engl. Token), der die erforderliche Information enthält (dies entspricht etwa einem "individuellen Türschlüssel").
- Durch *Wissen*, über das nur die betreffende Person verfügen kann (Ein Passwort oder PIN-Code).
- Durch *Eigenschaften*, die die Person besitzt (biometrische Merkmale).

Da ein Gegenstand gestohlen werden kann und auch Wissen transferierbar ist, finden sich häufig Kombinationen der genannten Merkmale.

Im Internet haben sich heute elektronische Signaturen auf der Basis asymmetrischer Verfahren, konkret RSA, etabliert. Dabei setzt das Verfahren auf die bereits diskutierten Verschlüsselungs- und Hash-Verfahren auf:

Signaturverfahren

Die Verwendung von RSA zur Authentisierung von Dokumenten oder Kommunikationskanälen erscheint in vielerlei Hinsicht komplementär zur Verschlüsselung. Während diese nur das kodierte Dokument überträgt, beläßt es eine elektronische Unterschrift im Klartext (wie man es auch von einem unterschriebenen Schriftstück auf Papier erwarten würde). Zusätzlich wird jedoch mit dem Dokument die Unterschrift des Senders übertragen. Dabei wird vom Dokument ein Hash-Wert erzeugt und mit dem privaten Schlüssel des Dokumentes verschlüsselt. Dadurch sind zwei Eigenschaften sichergestellt:

1. Das Dokument kann nur von einer einzigen Person stammen, da nur diese über ihren eigenen privaten Schlüssel verfügt. Der Hash-Code ist damit fälschungssicher verschlüsselt.
2. Das Dokument kann von niemand anderem verfälscht worden sein, da dies anhand des privaten Schlüssels der Person erfolgen müßte.

Da der private Schlüssel des Senders symmetrisch zu seinem öffentlichen ist, kann jeder, der über letzteren verfügt, verifizieren, von wem das Dokument stammt. Technisch erfolgt dies durch Entschlüsseln des Hash-Wertes mit dem öffentlichen Schlüssel und durch erneutes Anwenden der Hash-Funktion. Sind beide auf diese Weise ermittelten Hash-Werte identisch, ist nachgewiesen, daß das Dokument so wie ursprünglich beim Sender vorliegt.

Wichtig ist hierbei noch einmal der Hinweis, daß für die Verschlüsselung und für das elektronische Signieren jeweils unterschiedliche Schlüssel eingesetzt werden:

- Zum Verschlüsseln der öffentliche Schlüssel des Empfängers und
- zum Unterschreiben der private des Senders.

Die anderen beiden der möglichen vier Kombinationen sind nutzlos.

Die Möglichkeiten, mit den bisher genannten Verfahren zu spielen und die sich daraus ergebenden Kombinationen finden sich überall im Internet wieder. Krypto-Programmierbibliotheken, wie z.B. im Java Development Kit

1.2 [Knud98] bieten eine Fülle von Kombinationsmöglichkeiten und Verfahren. Alle gängigen e-Mail-Anwendungen bieten heute einfache Benutzerschnittstellen zur Generierung und Verwaltung von Schlüsseln. Besonders PGP (Pretty Good Privacy) von Phil Zimmerman hat hier Berühmtheit erlangt, da es erstmals RSA in einer weltweit öffentlichen Form implementierte. Entsprechend verärgert waren denn auch die NSA und das FBI, so daß Phil Zimmerman aus diesem Grund einige Zeit im Gefängnis verbringen mußte.

XXX Signatur-Gesetz

→ Evtl. im juristischen Abschnitt unterbringen

Trotz der immer rasanteren Durchdringung des Internet durch Signatur-Verfahren und der Zuverlässigkeit seiner Algorithmen bleibt ein wesentliches Problem offen: Wie kann ein Teilnehmer sich darauf verlassen, daß der öffentliche Schlüssel, den er von einem anderen besitzt, auch wirklich dessen ist und nicht ein eingeschleuster eines hinterlistigen Bösewichts?

Diese Frage und die zur Lösung erforderlichen Technologien markieren den Übergang von reinen *Sicherheitsmechanismen* hin zu Fragen der *Vertrauensinfrastruktur*. Von nun an schwenken wir von einer rein technischen Betrachtung hinüber zur tatsächlichen Massennutzung dieser Verfahren im Internet mit allen daraus entstehenden organisatorischen Problemen. Eine wesentliche Rolle spielen dabei *Zertifikate*.

5.1.5 Zertifikate

Die abstrakteste Definition, die man für Zertifikate wählen kann, ist vielleicht folgende:

"Ein Zertifikat ist eine nachprüfbare Aussage einer Person über eine andere".

Hierbei sind verschiedene Variationen vorstellbar, von denen wir einige hervorheben wollen: Die "Person" ist nicht nur eine natürliche, sondern in den meisten Fällen eine juristische Person, d.h. ein Unternehmen oder eine Behörde. Diese Person spielt die Rolle des *Herausgebers* oder *Erstellers*. Die Aussage beschreibt üblicherweise einen Zustand, ein Besitzverhältnis oder eine andere Eigenschaft Dritter. Schließlich bedeutet nachprüfbar, daß die Aussage nicht mündlich ausgesprochen wurde, sondern aufgrund der Schriftform durch Unterschriften, Stempel, Wasserzeichen, Siegel, Materialeigenschaften etc. verifizierbar ist. Gleiches gilt für Zertifikate in elektronischer Form. In jedem Fall ist ein Zertifikat leicht transportierbar und durch andere Personen verifizierbar. Dabei sind die weiteren Rollen definiert: Der *Besitzer* des Zertifikats ist meistens auch Nutznießer der im Zertifikat enthaltenen Aussage, während der *Prüfer* es verifiziert. Prüfer und Herausgeber können die gleiche Person sein. Wichtig ist ferner, daß ein Zertifikat auch außerhalb des "Dunstkreises" des Herausgebers – also in dessen Abwesenheit – leicht verifizierbar ist. Unter den Begriff des Zertifikats wollen wir ebenfalls Gutscheine subsumieren. Diese werden nur einmal beim Prüfer eingelöst und anschließend entwertet, während andere über längere Perioden hinweg oder sogar ewig Gültigkeit besitzen und beliebig oft vorgelegt werden können.

Beliebig viele konkrete Beispiele lassen sich im täglichen Leben finden: Angefangen beim Verzehrutschein eines Fast-Food-Restaurants oder dem einer Buchhandlung über Theatertickets, über die Urkunde der Handwerkskammer zur bestandenen Gesellenprüfung bis hin zu Geldscheinen oder Grundbucheinträgen haben wir es immer wieder mit Zertifikaten zu tun. In der Online-Welt finden wir Zertifikate für den Authentizitätsnachweis öffentlicher Schlüssel (heute die häufigste Anwendung) oder auch ansatzweise im Bereich von Qualitätszertifikaten ("Best Home Page", "Cool Java Applet" etc.). In diesem Bereich besteht jedoch noch keine auf öffentlichen Schlüsseln basierende Infrastruktur.

Bereits am hier gezeigten Spektrum kann man erkennen, daß die Eigenschaften "Wert des Gegenstands", "Aufwand zur Fälschungssicherung", "Vertrauenswürdigkeit des Herausgebers" nicht beliebig sind. Während das Theaterticket vielleicht noch mit einem Fotokopierer gefälscht werden kann, ist dies bei Geldscheinen oder Urkunden aufgrund der zusätzlichen physikalischen Eigenschaften nicht möglich.

Ausgehend von der zunächst primären Verwendung für öffentliche Schlüssel, definiert das deutsche Signaturgesetz ein Zertifikat wie folgt:

"Ein Zertifikat [...] ist eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat)." [SigG, §2(3)]

Die letztgenannten Anwendungen würden ein entsprechendes Attribut-Zertifikat erfordern (siehe auch weiter unten).

PKI - Public Key Infrastructure

Im Internet werden elektronische Zertifikate heute für den Nachweis der Zugehörigkeit eines öffentlichen Schlüssels zu einer Person verwendet. Diese Sicherung ist von grundlegender Bedeutung, da zunächst keine Anhaltspunkte existieren, anhand derer man erkennen kann, daß der öffentliche Schlüssel einer anderen Person auch wirklich ihrer ist. Er könnte ja von einem Angreifer zugespielt worden sein, so daß alle Nachrichten, die dem eigentlichen Adressaten gesendet werden, vom Angreifer abgefangen und entschlüsselt werden (und nur von diesem). Natürlich könnte unser Kommunikationspartner uns per Post oder per Telefon seinen öffentlichen Schlüssel übermitteln, dies würde allerdings die Transaktionskosten unnötig erhöhen.

Die Internet-Lösung besteht daher im Einsatz einer vertrauenswürdigen dritten Partei (engl. Trusted Third Party, TTP). Im Internet hat sich bei der Verwaltung von Zertifikaten für öffentliche Schlüssel der Begriff der Zertifizierungsautorität durchgesetzt (engl. Certification Authority, CA). Diese genießt so hohes Vertrauen, daß ihre Aussagen von allen Nutzern als gültig angenommen werden können. Ein Aussage der CA kann damit also sein: "Dieser öffentliche Schlüssel gehört Michael Merz". Wird diese Aussage noch von der CA unterschrieben, liegen bereits die wesentlichen Merkmale eines elektronischen Zertifikats vor.

Die Aufgaben der CA liegen dabei in der Verwaltung von Zertifikaten. Dazu zählen folgende Funktionen:

- Einrichtung von Prozeduren zur Registrierung einer Person und ihres öffentlichen Schlüssels
- Schaffung eines Online-Dienstes zur automatischen Verifikation von Schlüsseln
- Verwaltung von Schwarzen Listen für ungültige Zertifikate

Bei der ersten Funktion ist es Aufgabe der CA, die Zugehörigkeit des Schlüssels zur Person sicherzustellen. Dies kann unterschiedliche drastische Maßnahmen erfordern, angefangen bei der Überprüfung der korrekten e-Mail-Adresse (Zertifikate auf diesem Niveau haben fast keinen praktischen Wert und sind in der Regel kostenlose "Köderangebote" großer CAs) über das persönliche Einreichen auf Diskette (dabei ist ein Personalausweis vorzulegen) bis hin zur Zusammenarbeit mit Wirtschaftsinformationsdiensten, die den Lebenslauf, familiäre und berufliche Beziehungen, Sozialversicherungsnummern sowie Vermögensverhältnisse etc. recherchieren.

VeriSign, eine der größten CAs in den USA gibt beispielsweise Zertifikate unterschiedlicher Klassen heraus. Jede Klasse ist dabei mit einem anderen Zuverlässigkeits- und Haftungsniveau verbunden:

Tabelle XXX: Zertifikatklassen von Verisign

Zertifikatsklasse	Client/Server	Kosten für den Zertifizierten	Haftung seitens Verisign
Klasse 1:	Client	0	100,-- USD
Klasse 2:	Client	19,95 USD p.a.	5.000,-- USD
Klasse 3:	Client	290,-- USD 1. Jahr, 75,-- danach	100.000,-- USD
Klasse 4:	Server	290,-- USD 1. Jahr, 75,-- danach	100.000,-- USD

Zertifikate können online erstellt und erworben werden. Es ist wichtig, nochmals darauf hinzuweisen daß Zertifikate der Klasse 1 keinen praktischen Wert haben – im Gegenteil, sie suggerieren dem unbedarften Teilnehmer eher eine Sicherheit, die mangels Verifizierbarkeit gar nicht gegeben sein kann. Aus diesem Grund ist die Schaffung eines Mindeststandards für die Verfahrensregeln der Zertifizierung von elementarer Bedeutung. Zu diesem Zweck wurde in Deutschland das Signatur-Gesetz (SigG) verabschiedet, welches über nachgeschaltete Verordnungen und Direktiven einen rechtlichen Rahmen zur Einhaltung des erforderlichen Sicherheitsstandards schafft (siehe dazu auch XXX).

Unabhängig von der Qualität der Zertifikate ist jedoch die Prozedur ihrer Erteilung. Diese wird im folgenden kurz am Beispiel von VeriSign, einer der bedeutendsten CAs dargestellt. Dabei wird der Web-Browser des Benutzers eingesetzt, um folgende Schritte durchzuführen:

1. Zertifikatsklasse auswählen (1 oder 2).
2. Erforderliche Dokumente des Antragstellers liefern. Im Falle der Klasse 1: sind Vorname oder Alias, Nachname sowie die e-Mail-Adresse anzugeben. Für ein Zertifikat der Klasse 2 sind folgende Daten zu nennen: E-Mail-Adresse, Vorname, Nachname, evtl. mittlere Initialen, Titel, Postadresse, Apartment-/Hausnummer, Postleitzahl, Stadt, Region, Land, Geburtstag, Sozialversicherungsnummer, Führerscheinnummer (wichtig in den USA), private Telefonnummer, Vorname des Ehegatten, Arbeitgeber, vorherige Wohnadresse. Nicht alle Informationen werden validiert, VeriSign behält sich vor, welche.

3. Im nächsten Schritt sind Zahlungsinformationen einzutragen (Kreditkartennummer etc.).
4. Anschließend werden die bisher eingetragenen Daten dem Antragsteller nochmals zur Verifikation angezeigt.
5. Bevor der technische Prozess der Schlüsselgenerierung einsetzt, fordert VeriSign noch die Zustimmung des Antragstellers zu ihren Allgemeinen Geschäftsbedingungen und Verfahrensregeln. Dieses 90 Seiten lange Dokument wird dem Benutzer als HTML-Text angezeigt.
6. Jetzt wird das Formular zur Schlüsselerzeugung angezeigt. Dabei erfolgt die Schlüsselgenerierung "hinter den Kulissen" des Browsers. Zu diesem Zweck existiert ein HTML-Tag <KEYGEN>:

```
<KEYGEN TYPE=„hidden“ NAME=„name“ VALUE=„challenge string“>
```

7. Der öffentliche Schlüssel wird nun an den Web-Server der CA gesendet und der private auf der lokalen Festplatte gespeichert. Schließlich erstellt die CA ein Zertifikat für den Schlüssel und sendet dieses an den Benutzer per e-Mail zurück. Außerdem erfolgt ein Eintrag in das öffentliche Verzeichnis der CA, so daß es von Dritten jederzeit geladen werden kann.
8. Hat der Benutzer das Zertifikat erhalten, kann er es im Browser registrieren, damit es zur Verfügung steht, wenn ein Kommunikationspartner es anfordert.

Der gesamte Ablauf erfolgt SSL-geschützt mit Authentifizierung des Servers und verschlüsselter Datenübertragung.

Zertifikate nach dem X.509v3-Standard

Nachdem wir nun Zertifikate aus der Perspektive des Benutzers untersucht haben, wollen wir einen Blick auf ihre technische Realisierung werfen. Dabei stehen drei Aspekte im Vordergrund: Die Datenstruktur eines Zertifikats, seine Verwaltung seitens der CS sowie die Kommunikation zwischen Benutzer und CA.

Im wesentlichen dient ein bereits etwas betagter CCITT/ISO-Standard als Grundlage zur Verwaltung von Zertifikaten: Der X.500 Verzeichnisdienst. Dieser wurde Ende der 80er Jahre entwickelt (also lange vor dem WWW), um Teilnehmerinformationen in einheitlicher Weise online zu verwalten und für andere Benutzer oder Anwendungen zugänglich zu machen. Dabei waren die folgenden Elemente die wesentlichen Bestandteile des X.500-Standards:

- Ein **einheitlicher, globaler Namensraum** für Verzeichnisse und Datenobjekte. Hierbei war der X.500-Standard losgelöst von der heute im Internet gegebenen Namenshierarchie für Domänen und Rechner. Stattdessen wurde eine Schema definiert, welches festlegt, nach welchen Regeln Einträge für Länder, Organisationen, Unterorganisationen etc. im globalen Namensraum erfolgen konnten. Die dafür verwendete Syntax entstammt dem X.400-Standard der CCITT für e-Mails, der heute keine praktische Bedeutung mehr hat. Seine Syntax zur Benennung von X.500-Objekten lebt jedoch fort. Beispielsweise würde mein Name im X.500-Verzeichnis etwa folgendermaßen aussehen: "C=DE, O=PontonHamburg, OU=ECommerce, CN=Merz". Dabei legen die Kürzel C, O, OU, CN entlang der Verzeichnishierarchie den Knotentypen fest (Country, Organization, Organizational Unit, Common Name). Das X.500-Namensschema erlaubt hier beispielsweise eine beliebige "Verlängerung" des OU-Teils, so daß auch größere Organisationen ihre Struktur über mehrere Hierarchieebenen abbilden können.
- Ein **einheitliches (d.h. standardisiertes) Benennungsschema** für Einträge in dieser Verzeichnisstruktur. Unabhängig von der Verzeichnisstruktur, können den Knoten dieser Hierarchie Objekte zugeordnet werden. Diese Objekte setzen sich aus beliebig vielen Teilobjekten oder elementaren Datentypen zusammen und sind hinsichtlich ihres Typs ebenfalls zentral standardisiert. Allerdings kann ein Teilnehmer über die standardisierten Typen hinaus beliebige eigene definieren, die dann natürlich nicht von X.500-konformen Anwendungen interpretiert werden können (z.B. zur Visualisierung). Typische Objekttypen sind Benutzernamen, -adressen, Kommunikationspräferenzen sowie beliebige andere Profilinformatoren. Unter anderem zählen dazu auch öffentliche Schlüssel und deren Zertifikate. Heute hat sich die Bedeutung von X.500 im wesentlichen reduziert auf standardisierte Zertifikate nach dem Teilstandard X.509.
- Festlegung eines **einheitlichen Protokolls** zur Kommunikation zwischen Benutzern und X.500-Verzeichnisdienst sowie zwischen Verzeichnis-Servern. Das globale Verzeichnis kann aus Gründen der Skalierbarkeit nicht von einem einzelnen Rechner verwaltet werden. Folglich war eine Aufteilung nach Teilbäumen des Verzeichnisses auf beliebig viele Rechner erforderlich, ohne jedoch dem Benutzer Einblick zu gewähren, mit welchem tatsächlichen Server er kommuniziert. Während er beim WWW immer informiert ist, zu

welchem Server die aktuelle Verbindung besteht, reicht beim X.500 die Verteilungstransparenz erheblich weiter. Hierbei bestand die Anforderung, die möglicherweise komplexen Kommunikationsbeziehungen zwischen X.500-Browser und -Server zu verbergen. Dazu wurden insbesondere zwei Protokolle eingesetzt: DAP (Directory Access Protocol) und DSP (Directory Service Protocol XXX???)

X.509 Format für Zertifikate

Von der gesamten Mächtigkeit (und dem zigmillionenschweren Forschungsaufwand) des X.500-Standards ist immerhin noch X.509 (ISO Authentication Framework, [CCITT89]) in die Praxis eingeflossen: Dieser liegt in drei Versionen vor, von denen die letzte insbesondere für Zertifizierungsaufgaben, die über öffentliche Schlüssel hinausgehen, relevant ist.

Ein X.509-Zertifikat setzt sich aus folgenden Komponenten zusammen:

Tabelle XXX: Aufbau eines X.509-Zertifikats

Komponente	Beschreibung
Versionsnummer	1 bis 3
Seriennummer des Zertifikats	Eindeutig für jede CA
Algorithmus-ID	Verwendeter Algorithmus für die Signatur, z.B. DSA
X.500-Name der CA (Issuer Name)	Z.B. "C=US, O=VeriSign"
Gültigkeit (Validity)	Beginn ("Not before <Date>") und Ablauf ("Not after <Date>") der Gültigkeit
Gegenstand (Subject)	Der Benutzername
Subject Public Key Information	Algorithmus, Parameter & der öffentliche Schlüssel selbst
Signatur der CA	Die Unterschrift des öffentlichen Schlüssels durch die CA
Issuer's Unique Identifier (seit Version 2)	Eindeutige Kennung der CA (inkl. WWW-Adresse)
Subject Unique Identifier (seit Version 2)	Im Falle anderer Aufgaben als öffentliche Schlüssel zu zertifizieren, wird hiermit festgelegt, um welche Art von Zertifikat es sich hierbei handelt.
Extensions (seit Version 3)	Zertifikate können mit Einschränkungen und Bedingungen versehen werden. Dafür erforderliche zusätzliche Informationen können in dieser Komponente abgelegt werden.

Das deutsche Signaturgesetz hat den X.509-Standard übernommen. Der Wortlaut zum Inhalt von Zertifikaten lautet [SigG97]:

§ 7 Inhalt von Zertifikaten

(1) Das Signaturschlüssel-Zertifikat muß folgende Angaben enthalten:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß,
2. den zugeordneten öffentlichen Signaturschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der öffentliche Schlüssel des Signaturschlüssel-Inhabers sowie der öffentliche Schlüssel der Zertifizierungsstelle benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen der Zertifizierungsstelle und
7. Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist.

Der PKCS-Industriestandard

Der Public Key Cryptography Standard wurde in Kollaboration mit Industriepartnern von RSA entwickelt. Er setzt sich bislang aus zehn Standarddokumenten zusammen, von denen im folgenden die wichtigsten aufgelistet sind:

- PKCS #1: RSA Encryption Standard. Spezifiziert das RSA Verschlüsselungsverfahren.
- PKCS #3: Spezifiziert das Verfahren nach Diffie-Hellman zur Einigung auf ein Schlüsselpaar.
- PKCS #6: Extended-Certificate Syntax legt die Syntax fest, die bei der Erweiterung von Zertifikaten (X.509v3) verwendet werden sollte.
- PKCS #9: Spezifiziert bestimmte Attributtypen, die für Zertifikatserweiterungen verwendet werden können.
- PKCS #10: Legt die Syntax fest für die Abfrage von Zertifikaten (Certificate Request).

Management von Zertifikaten

Wenn nun das Kommunikationsprotokoll für die Registrierung von Zertifikaten sowie deren Struktur festgelegt sind, fehlt noch eine wesentliche Komponente: Wie können zwei Kommunikationspartner ihre jeweiligen Zertifikate verifizieren, wenn sie vorher noch nie etwas voneinander gehört hatten und evtl. sogar ihre jeweiligen CAs einander unbekannt sind?

Theoretisch gibt es im wesentlichen drei Modelle, nach denen CA oder auch Personen sich untereinander zertifizieren können, so daß durch das Verfolgen dieser Vertrauensbeziehungen von einer Instanz auf die nächste geschlossen werden kann:

- **Trust Network.** Hierbei zertifizieren sich die Besitzer öffentlicher Schlüssel gegenseitig. Jeder Besitzer kann sich dabei beliebig viele Zertifikate befreundeter Personen erstellen lassen. Die Annahme ist, daß sich bei einer hinreichenden Durchdringung aller Personen immer ein Pfad zwischen zwei beliebigen ermitteln läßt. Es hängt letztlich von der Vertrauenswürdigkeit vieler einzelner Personen ab, ob man den öffentlichen Schlüssel eines Unbekannten als authentisch erachtet oder nicht. Dabei ist die Länge der Vertrauenskette nicht kontrollierbar. Außerdem kann in der Praxis nicht sichergestellt werden, daß es immer einen Pfad zwischen zwei Personen gibt. Schließlich existieren weder normierte Verfahrensregeln, nach denen die Identität einer Person überprüft wird (z.B. Überprüfung der Personalausweisnummer), noch besteht ein gesetzliches Rahmenwerk, das mögliche Verstöße justiziabel macht.
- **Reine Hierarchie.** Hierbei wird angenommen, daß weltweit eine einzige Wurzel-CA andere CAs, z.B. nationale Wurzel-CAs zertifiziert. Diese wiederum können untergeordnete CAs zertifizieren, so daß sich eine beliebige tiefe Hierarchie ergeben kann. Tritt man mit einem Benutzer in Verbindung, kann entlang dieser Zertifizierungshierarchie – notfalls bis zur Wurzel-CA – ermittelt werden, ob die jeweiligen Zertifikate gültig sind. Der Vorteil besteht hier in der – im Gegensatz zum Trust Network – sehr statischen Struktur, da mindestens die oberen 2-3 Ebenen sich im Laufe der Jahre kaum ändern werden. Damit sind diese CAs wesentlich besser kontrollierbar. Dies gilt sowohl hinsichtlich der Einhaltung von Sicherheitsmaßnahmen bei der Etablierung einer CA als auch für den laufenden Betrieb der Zertifizierung. Der Nachteil besteht jedoch in der reduzierten Autonomie nationaler Gesetzgebungen sowie in einer möglicherweise zu tiefen Hierarchie, die eine zu hohe Last durch die häufiger erforderlichen Verifikationsprozeduren bewirkt.
- **Wald.** Hier existiert keine einzelne Wurzel-CA, sondern beliebig viele – auch national. Dabei könnten die oberen 2-3 Hierarchie-Ebenen durch eine gegenseitige Zertifizierung der CAs verkürzt werden. Während eine CA des reinen Hierarchiemodells nur untergeordnete zertifiziert, gilt dies beim Wald auch für Schwester CAs. Dieses Modell ist wesentlich praktikabler, da es die Autonomie von CAs erhöht, sowohl bez. der Etablierung einer CA als auch bez. ihrer Querbeziehungen. Dieses Modell erlaubt ferner auch die Entwicklung unabhängiger, nationaler Regulierungen, so daß sich im Wettbewerb dieser organisatorisch-juristischen Rahmenwerke "erfolgreiche" Modelle besser durchsetzen können.

CA-Software steht heute als Produkt bei verschiedenen Anbietern zur Verfügung:

- Entrust/Commerce CA (www.entrust.com)
- CyberTrust Certificate Management System (www.bbn.com/products/security/cytrust/caprods.html)
- Netscape XXX (www.netscape.com/XXX)

Beispiel zum hierarchischen Modell

Stellen wir uns vor, daß Sie mit mir ein Geschäft durchführen wollen (z.B. ein Buch kaufen) . Sie (L=Leser) sind bei Thawte (www.thawte.com) zertifiziert und ich (M) bei der CA des DFN (www.pca.dfn.de). Ihre Software muß auf irgendeine Weise meinen öffentlichen Schlüssel verifizieren können. Dazu findet folgende Kommunikation statt:

1. L fragt M's Zertifikat seines öffentlichen Schlüssels nach.
2. M liefert sein von "DFN" herausgegebenes Zertifikat an L.
3. L's Software prüft, ob sie die betreffende CA "kennt", d.h. ihren öffentlichen Schlüssel besitzt (dieser ist zur Verifikation von M's Zertifikat erforderlich). Dies ist jedoch nicht der Fall.
4. Da M's Zertifikat die WWW-Adresse der DFN-CA enthält, wendet sie sich im nächsten Schritt an die betreffende CA und lädt deren öffentlichen Schlüssel, mit dem sie die Gültigkeit von M's öffentlichen Schlüssel verifiziert.
5. Allerdings ist die DFN-CA L's Software noch unbekannt und damit nicht vertrauenswürdig, folglich beginnt das Spiel bei Schritt 1 von vorne. Dabei wird eine Hierarchie nach oben verfolgt, bis eine für L's Software wohlbekannte CA erreicht wird. Diese CA ist nach dem rein hierarchischen Modell die Wurzel des minimalen Teilbaumes, der beide Teilnehmer enthält.

Abb. XXX verdeutlicht noch einmal das Verfolgen von Zertifikaten vom Benutzer "Michael Merz" über zwei CAs bis hin zur VeriSign als Wurzel.⁶

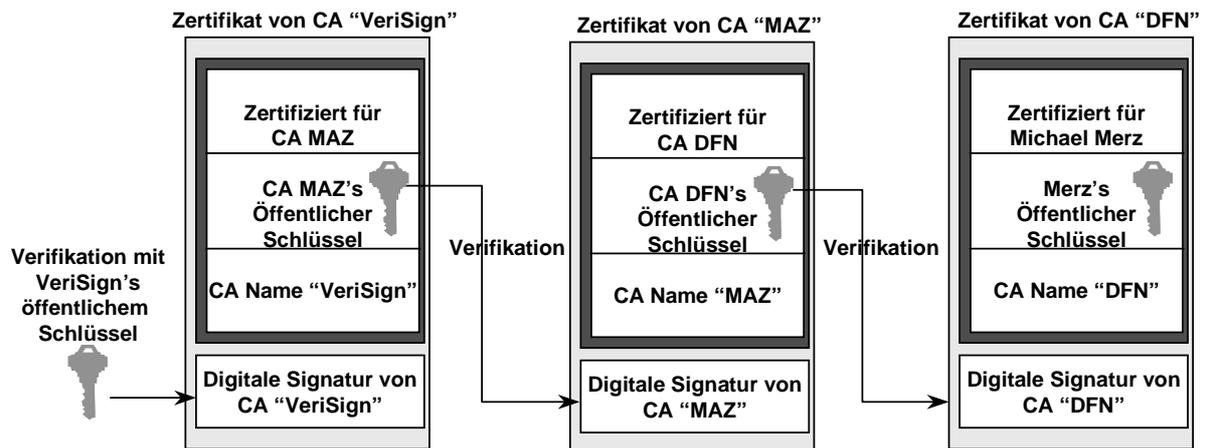


Abb. 7: Zertifizierungshierarchie

Schwarze Listen

Leider kann es trotz aller Sicherheitsvorkehrungen schnell passieren, daß ein Teilnehmer seine SmartCard verliert oder ein Angreifer seinen privaten Schlüssel erlangt. Dies erfolgt üblicherweise lange vor dem Ablauf der Gültigkeit des Zertifikats, so daß dem Angreifer Tür und Tor offenstehen, die Authentizität des anderen Teilnehmers vorzutäuschen.

Diese Angriffsszenarien können heute nicht a priori vermieden werden, daher liegt der Schwerpunkt der technologischen Unterstützung bei der Erkennung solcher Fälle und der Schaffung eines Informationssystems, das entsprechende Zwischenfälle schnell anderen Teilnehmern meldet. Diesem Zweck dienen *Schwarze Listen* bzw. *Certificate Revocation Lists (CRLs)*. CRLs werden von jeder CA für die von ihr zertifizierten Teilnehmer vorgehalten. Wenn der Fall eintritt, daß ein Teilnehmer seinen öffentlichen Schlüssel als ungültig erklärt, wird dessen Seriennummer zusammen mit einem Zeitstempel und weiteren Informationen in die CRL eingetragen. Die gesamte CRL wird selbst regelmäßig von der CA unterschrieben, so daß für andere Teilnehmer erkennbar ist, daß sie nicht von Betrügern eingeschleppt worden sein kann. Abb. XXX zeigt die Struktur einer CRL.

⁶ Dies ist nur ein Beispiel, natürlich ist in der Praxis nirgendwo vorgeschrieben oder vereinbart, daß eine CA immer als Wurzel dient.

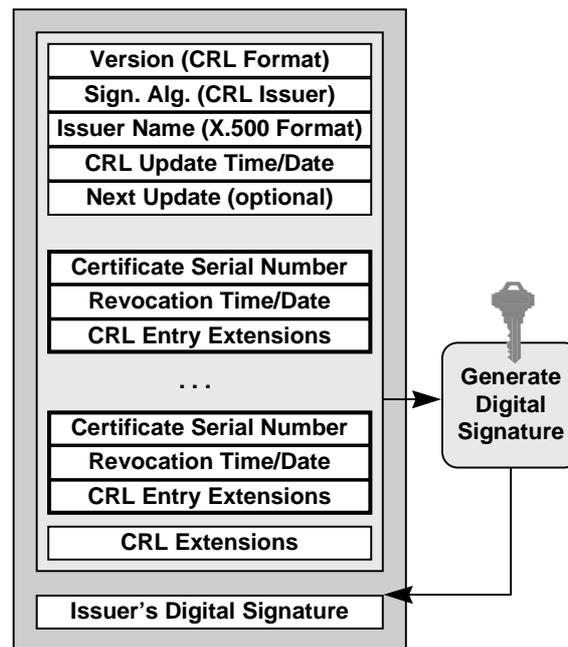


Abb. 8 Eine Sperrliste für X.509 Zertifikate

Das grundsätzliche Problem bei CRLs liegt in der Verzögerung zwischen dem Vorfall (z.B. Verlust des privaten Schlüssels) und der tatsächlichen Verwendung der CRL-Einträge. Die Gesamtverzögerung setzt sich aus folgenden Phasen zusammen:

1. **Bekanntwerden des Vorfalls durch den Teilnehmer selbst.** Vom Kreditkartenverlust her weiß man, daß Stunden bis Tage vergehen können, bis dieser entdeckt wird. Schlimmer noch: Wenn der private Schlüssel auf elektronischem Wege gestohlen wurde, ist dies gar nicht erkennbar!
2. **Meldung des Verlusts** (Revocation Request). Nicht immer ist der Teilnehmer Online oder verfügt über die nötige Information zur Meldung des Verlusts. Dies bewirkt eine weitere Verzögerung
3. **Eintragung in die CRL** (Revocation Publication). Auch hier kann noch eine gewisse Verzögerung seitens der CA auftreten.
4. **Abruf der CRL-Einträge durch andere Teilnehmer** (CRL Download). Dies erfolgt eher im Tagesrhythmus als stündlich, folglich kann die weitere Verzögerung zu fast einem Tag führen, wenn die Veröffentlichung kurz nach dem letzten Abruf stattfindet.

Insgesamt hängt es also von verschiedenen Einstellungen und Parametern der beteiligten Softwaresysteme ab, wie hoch die Gesamtverzögerung tatsächlich ist. Pessimistischerweise sollte man sie jedoch eher in Tagen als in Stunden messen. Da dies im Falle eines Diebstahls dem Angreifer durchaus bewußt sein dürfte, wird er versuchen, möglichst schnell Schaden anzurichten. Vermutlich wird er dazu – bei geeigneter Vorbildung – nicht länger als ein paar Minuten benötigen. Schon dies spricht für ein anderes Modell als das der CRL. Nimmt man noch zusätzlich an, daß im Rahmen des CRL-Modells zur Reduzierung von Schäden alle 10 Minuten der Download erfolgt, kann es durchaus sein, daß der Aufwand niedriger ist, wenn bei jeder Kommunikationssitzung mit einem Partner, dessen Zertifikat erneut von der CA abgerufen wird. Wenn eine solche Kommunikation alle 10 Minuten erfolgt, mag zwar der Rhythmus der gleiche sein, jedoch erfordert ein einzelnes Zertifikat weniger Rechen- und Kommunikationsaufwand als eine komplette CRL.

Dieser Ansatz wird im allgemeinen "Instant Certificates" genannt, d.h. immer dann, wenn der öffentliche Schlüssel eines Partners verwendet wird, erfolgt ein Zugriff auf die CA. Für die CA ergibt sich dabei das Problem, daß jedesmal eine neue Signatur erstellt werden muß. Dies erfordert auf einem schnellen Pentium-II ca. 1 Sekunde. Nimmt man an, daß durch eine CA 100.000 Personen zertifiziert sind und diese um 11.00 Uhr vormittags sich auf dem Höhepunkt ihrer Kommunikationsaktivität befinden (d.h., 10% kommunizieren so, daß 1x pro Minute ihr Zertifikat abgerufen wird), erfordert dies 10.000 Sekunden pro Minute Rechenzeit – also über 166 Pentium-II. Glücklicherweise kann dies durch Hardware etwa um den Faktor 300 beschleunigt werden, was jedoch bedeutet, daß jede CA sich schon aus technischen Gründen (abgesehen von regulatorischen) eine entsprechende

Hardware anschaffen sollte. Entsprechende Systeme werden heute als Steckkarten für den PCI-Bus angeboten oder zukünftig auch als PC-Card (XXX → z.B. IBM-CryptoCard).

Es bleibt jedoch festzuhalten, daß damit noch nicht dem Diebstahl als solchem vorgebeugt werden kann. Dazu sind weitere Verfahrensregeln erforderlich, die einen Verlust durch Diebstahl verhindern oder zumindest reduzieren helfen. Eine wesentliche dieser Anforderungen ist die Voraussetzung hardwarebasierter Sicherheitstechnik, wie z.B. SmartCards.

Verfahrensregeln

Nachdem wird uns nun mit den sicherheitstechnischen Grundlagen zur Schaffung einer Vertrauensinfrastruktur beschäftigt haben, sollen abschließend noch einige organisatorische Aspekte beleuchtet werden.

Rein technisch könnte eine CA auch von der Mafia betrieben werden. Ihre Vertreter verfügen über (mindestens ;-) eine Personalausweisnummer und weitere Informationen, die sie zum Betrieb einer CA qualifizieren können. Um diesem Fall vorzubeugen, sind sehr restriktive Auflagen durch den Gesetzgeber und die an der Umsetzung beteiligten Instanzen ausgearbeitet worden.

Signaturgesetz und Signaturverordnung legen bereits einige konkrete Maßnahmen fest, die einerseits den Betreibern von CAs recht hohe Kosten aufbürden, andererseits aber auch als vertrauensschaffende Voraussetzungen erforderlich sind. Beispiele für diese Maßnahmen sind:

- Polizeiliches Führungszeugnis für CA-Betreiber und deren Personal,
- Beteiligung von Beamten der zuständigen Behörde bei Erteilung von Genehmigungen für den Betrieb einer Zertifizierungsstelle, Ablehnung eines Antrags auf Erteilung einer Genehmigung, der Rücknahme oder den Widerruf einer Genehmigung, die Ausstellung von Zertifikaten für CAs, Überprüfung von Prüfberichten und deren Bestätigungen oder auch die Übernahme der Dokumentation bei Einstellung der Tätigkeit einer CA.
- Einhaltung des Datenschutzgesetzes mit der Maßgabe, daß die zuständige Behörde Prüfungen vornehmen darf, auch wenn keine Anhaltspunkte für eine Verletzung von Datenschutzvorschriften vorliegen.
- Berücksichtigung von geeigneten Sicherheitsmaßnahmen bei der Erstellung des Sicherheitskonzeptes der CA. Diese müssen konform sein zum Maßnahmenkatalog des BSI (Bundesamtes für Sicherheit in der Informationstechnik). Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.
- Dokumentation von Sicherheitsrichtlinien, Zertifizierungsvorgängen, Kundendaten und Pseudonymen für einen Zeitraum von mindesten 35 Jahren. Dabei sind digitale Dokumente von der CA zu signieren.
- Die technischen Komponenten, welche zur Erstellung von Signaturen eingesetzt werden, müssen restriktiven technischen und ergonomischen Anforderungen genügen. Auch wenn nicht ausgeschlossen ist, daß reine Softwarelösungen diesen Anforderungen gerecht werden, scheinen jedoch – zumindest schon aus ergonomischen Gründen – Hardwarelösungen wie z.B. SmartCards den Anforderungen besser gerecht zu werden.

Eine weitere Maßnahme, die nicht in der SigV direkt gefordert wird, ist z.B. die Aufteilung der Tätigkeit einer CA auf mehrere Organisationen, die sich für die jeweiligen Teilaufgaben besonders eignen. So könnte Bearbeitung von Anträgen etwa von einer Behörde oder Handelskammer vorgenommen werden, die intern über erforderliche Informationen zur Identifikation des Antragstellers verfügt. Der technische Betrieb der CA als Online-Dienst könnte hingegen von einem Telekommunikationsunternehmen oder einem ISP durchgeführt werden. Schließlich könnte auch eine Bank involviert sein, z.B. für Teilaufgaben der Kreditkartenzertifizierung.

XXX ...

Weitere Anwendungen für Zertifikate

Zertifikate wurden bisher nur im Kontext der Public-Key-Infrastrukturen erörtert. In zukünftigen Electronic-Commerce-Anwendungen sind jedoch verschiedene Nutzungsformen denkbar, für die Attribut-Zertifikate verwendet werden können:

- ◆ **Vollmacht.** Nehmen wir an, eine Person, die als Vertragspartei beteiligt ist an der Unterzeichnung eines Vertrages, autorisiert eine zweite, diesen zu unterschreiben. Dies kann ad hoc geschehen oder aber auch bei einer CA für einen längeren Zeitraum hinterlegt sein. Eine solche Vollmacht kann pauschal oder qualifiziert sein.

Sie kann sich z.B. nur auf das Unterzeichnen von Verträgen beziehen oder darüber hinaus auch Bedingungen definieren, unter denen die Vollmacht gültig ist. Denkbar ist hier das Unterzeichnen in Verbindung mit einem anderen Bevollmächtigten (4-Augenprinzip). Prinzipiell ist für jedes Unternehmen eine entsprechende Autorisierung mit Hilfe eines Attribut-Zertifikates erforderlich, wenn zuverlässig und zeitgerecht verifiziert werden soll, ob einer Person Vertretungsbefugnis für ihr Unternehmen erteilt wurde.

- ◆ **Prädikate.** Heute finden wir auf bekannten Web-Seiten etliche Online-Prädikate der Form "Best Home Page of the Year", "Cool Java Applet" oder "ComputerMagazin Award" etc. Diese Prädikate sind zwar Zertifikate, jedoch mangeln sie an der erforderlichen Präzision und Verifizierbarkeit. Letztlich ist es eine Frage des Vertrauens, ob hier Etikettenschwindel betrieben wird oder der Betreiber tatsächlich Preisträger ist. Unter der Annahme, daß für bestimmte Kategorien eine Stufung von Qualitätsmerkmalen formalisiert werden kann, lassen sich derartige Zertifikate durch Nutzung der "Extensions"-Komponente im X.509-Standard relativ leicht realisieren.
- ◆ **Object Signing.** Java Applets oder Active-X-Komponenten lassen sich bereits heute signieren. Dafür werden übliche Verfahren der Public-Key-Kryptographie verwendet. Neben dem Authentizitätsnachweis kann ein mitgeliefertes Attribut-Zertifikat jedoch auch noch weitere Eigenschaften attestieren. Beispiele wären etwa: "JavaSoft 100% Java Compliant" oder "Compliant with Oracle Cartridge Specification".
- ◆ **Rating.** Neben Objekten und Software lassen sich auch Betreiber von Web-Services hinsichtlich verschiedener Qualitätsmerkmale zertifizieren: Beispiele sind auch hier "99.9% Verfügbarkeit" oder "Jugendfreier Webserver". Insbesondere im Bereich pornographischer Web-Sites ist im Laufe der letzten Jahre der PICS-Standard entstanden, der – allerdings als Einbettung in Web-Seiten – in Form einer freiwilligen Selbstkontrolle ein Rating-Schema definiert hat. Auch hier ist eine Umsetzung des Standards auf Attribut-Zertifikate, die von unabhängigen Dritten vergeben werden, denkbar.
- ◆ **Berufsqualifikationen.** Schließlich fallen mir noch Universitätsdiplome, "Microsoft Certified Engineer"-Zertifikate oder einfach Teilnahmebestätigungen und Schulungsmaßnahmen als weitere Beispiele ein.

Leider ist es mit meiner Kreativität an dieser Stelle zu Ende – sicherlich kennt jeder von Ihnen weitere Situationen im Leben, in denen die X.509-Infrastruktur für klassische oder neuartige Zwecke eingesetzt werden könnte. Dabei sind jedoch vor allem zwei Faktoren zu beachten:

1. Wieviel kostet die Infrastruktur, wer bezahlt diese und rechnet sich dies für alle Beteiligten?
2. Standardisierung der Attribute. Wie bereits aus den Beispielen erkennbar, sind jeweils völlig andere Daten und Datentypen zu standardisieren. Insbesondere im Internet stellt die Standardisierung einen internationalen, und damit recht trägen Vorgang dar (wenn es ein de-jure-Standard sein soll). Daher meine Schätzung: Attribut-Zertifikate sollten wir nicht vor dem Jahre 2005 erwarten (und schon gar nicht im "Massenbetrieb").

Auswirkungen des Signaturgesetzes

Die Deutsche Telekom AG, Bonn, bietet als erstes deutsches Unternehmen Chipkarten an, die den Richtlinien des deutschen Signaturgesetzes entsprechen. Damit können Kunden auf elektronischen Daten rechtsverbindliche elektronische Signaturen leisten. Als Registrierungsagenturen werden die ca. 500 "T-Punkte" der Telekom eingesetzt. Zur Zeit liegt der einmalige Kaufpreis einer Karte bei 50 DM und der Jahresbeitrag für die Trust-Center-Dienstleistung bei 100 DEM. Zusätzlich wird noch ein Kartenlesegerät benötigt, das die Telekom im Verbund mit weiteren Sicherheitskomponenten unter dem Namen "Security First" für 299 DEM vertreibt.

Zusammenfassung

Wir haben Zertifikate als eines der Grundbausteine für eine sichere und vor allem vertrauenswürdige Abwicklung von Handelstransaktionen kennengelernt. Obwohl Zertifikate heute hinsichtlich ihrer technischen Infrastruktur als beherrschbar erscheinen, stellt sich jedoch die Frage, wie sie in das ökonomische Gefüge der NetworkEconomy passen. Faßt man den technischen und organisatorischen Aufwand zusammen, der für die Verwaltung von Zertifikaten erforderlich ist, kann man erkennen, daß sie zumindest auch absehbare Zeit nicht kostenlos sein werden.

Für mich als Buchautor würde es sich wahrscheinlich nicht lohnen, ein Electronic-Commerce-Buch über das Web zu verkaufen, wenn mich die Zertifizierung einige tausend Mark kosten würde.

Folglich ist eine Zertifizierungsinfrastruktur, wie sie unter den strengen Sicherheitsvorkehrungen des SigG zu erwarten ist, evtl. inkompatibel mit der "Free-Economy".

XXX

5.2 SmartCards

Alles, wozu SmartCards eingesetzt werden, läßt sich funktional auch auf andere Weise realisieren, z.B. auf dem PC. Worin liegt dann der Vorteil einer SmartCard? Während ein PC, eine Unix-Workstation oder ein PDA seine Innereien einem Eindringling offenlegt, ist dies physikalisch bei SmartCards unterbunden. Während ein Betriebssystem nur so sicher ist wie die Möglichkeit, daß sich ein Eindringling das Administratorenpasswort erschleicht, kann absolut niemand auf der Ebene der Hardware und der Software in das System eindringen. Nur über eine übersichtliche, wohldefinierte Schnittstelle kann ein Protokoll für den Austausch von Daten abgewickelt werden. Eine SmartCard ähnelt daher einer Workstation im Netzwerk, die durch ein gußeisernes Gehäuse und sicheres Kommunikationsprotokoll geschützt ist. Niemand kann sich einloggen, niemand kann frei auf den Speicher dieser Workstation zugreifen. Wenn dennoch ein physikalischer Angriff versucht wird, zerstört sich die Workstation eher selbst, als daß sie dem Angreifer Informationen preisgibt. Schließlich besitzt diese Workstation eine global eindeutige ID und ein Schlüsselpaar, dessen Geheimschlüssel irgendwo im Inneren der Workstation verborgen bleibt.

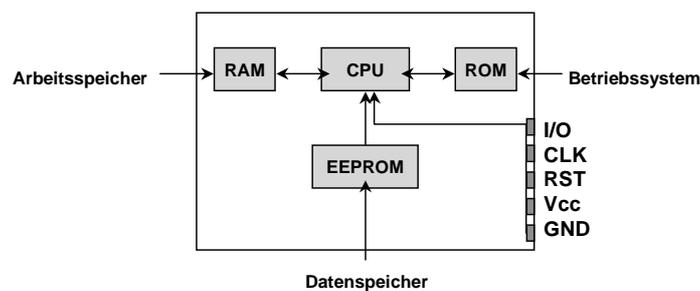


Abb. 9: Grundschema einer SmartCard

Im Gegensatz zur SmartCard besitzen einfachere *Chipkarten* lediglich einen Speicher mit wahlfreiem Zugriff. So kann jeder, der über das erforderliche Lesegerät verfügt, diese Information auslesen und sogar manipulieren, ohne daß dies hinterher erkennbar ist. Ein Beispiel für eine derartige Chipkarte ist die Krankenversichertenkarte. Die einzige Chance, bei Chipkarten ein gewisses Maß an Sicherheit zu gewähren, ist die Verschlüsselung der Daten mit einem symmetrischen Schlüssel (z.B. DES oder IDEA). Chipkarten erlauben eine Speicherkapazität von bis zu 32 Kilobyte. Schreib-/Lesegeräte sind für sie recht preiswert (≤ 50 Euro).

Noch weniger Schutz bieten *Magnetkarten*, die ebenfalls frei lesbar und wiederbeschreibbar sind. Zudem lassen sie sich mit einem Magneten auf einfache Weise unbrauchbar machen. Ihr einziger Vorteil liegt im extrem günstigen Preis (weniger als 0,5 Euro).

Im Umlauf sind des weiteren Chipkarten, deren Speicherzellen gezielt zerstört werden können. Die Telefonkarte folgt diesem Prinzip. Bei Einschieben der Karte in das Lesegerät wird die Anzahl der unzerstörten Einheiten angezeigt. Mit jedem Zeittakt erfolgt dann ein gezieltes Durchbrennen der jeweiligen Feinsicherungen.

Damit besitzt eine SmartCard folgende Eigenschaften, die für den Bereich des Electronic Commerce relevant sind:

- Eine SmartCard verfügt über einen eigenen Computer mit CPU, ROM, RAM, Einheiten zur Datenein- und -ausgabe sowie zusätzliche Module, die für kryptographische Verfahren verwendet werden (kryptographischer Koprozessor). Üblich sind heute 2-4 KB Ram, 24-36 KB Rom, bis zu einem MIPS Rechenleistung. Neuere Entwicklungen sehen sogar eine numerische Eingabetastatur auf der Karte vor.
- Eine SmartCard besitzt ein eigenes Betriebssystem, mit dessen Hilfe Programme ausgeführt, Daten und Software persistent in einem Verzeichnis gespeichert und die Kommunikation mit der Außenwelt abgewickelt werden kann. Üblicherweise steht der Karte ein hierarchisches Dateisystem zur Verfügung, mit dem Dateien wie unter einem PC-Betriebssystem verwaltet werden können.

- Eine SmartCard ist physikalisch gegen Angreifer geschützt. Weder über ihre Kontaktflächen, noch durch Abfräsen der Chipoberfläche können Informationen ausgelesen werden.

Das wichtigste Merkmal einer SmartCard ist ihr Geheimschlüssel, mit dem sie ausgeliefert wird. Er wird in der SmartCard erzeugt und kann damit von niemandem zugegriffen werden. Der kryptographische Koprozessor der Karte erlaubt dabei, RSA-Schlüssel mit bis zu 1024 Bit Länge zu generieren. Der korrespondierende öffentliche Schlüssel wird hingegen an den Benutzer ausgeliefert. Damit bestehen nun folgende Möglichkeiten:

- Daten und Programme können mit dem öffentlichen Schlüssel der SmartCard verschlüsselt und an diese übertragen werden. Damit ist sichergestellt, daß nur die Karte, für die die Daten vorgesehen waren, auch diese Informationen verarbeiten kann.
- Umgekehrt können Daten, die die Karte an Kommunikationspartner sendet, authentifiziert werden, indem die Karte diese mit ihrem Geheimschlüssel signiert.

Wenn nun zusätzlich sichergestellt werden kann, daß die Karte eindeutig mit einem Besitzer verbunden ist, so ist ein sicheres und einfach handhabbares Mittel zur Authentisierung der Person gegeben. Da sich die Verketzung zwischen Person und Signaturschlüssel durch Zertifizierungsauthoritäten sicherstellen läßt, ist jetzt der Kreis geschlossen, der für das Leisten einer elektronischen Signatur erforderlich ist. Da das Signieren nicht außerhalb der SmartCard erfolgen kann (dann wäre ja der geheime Schlüssel kurzfristig sichtbar), müssen die zu signierenden Daten an die Karte übermittelt werden. Dies erfolgt durch Generieren des Hash-Wertes auch außerhalb der Karte, so daß nur dieser zum Verschlüsseln übergeben wird. Außerhalb der Karte kann die Authentizität der Signatur jederzeit verifiziert werden.

Auch für das verschlüsselte Übertragen von Daten an die Karte gibt es interessante Anwendungen: Man stelle sich vor, ein Least-Cost-Router muß regelmäßig mit Informationen über die günstigsten Gebühren der Telefonprovider versorgt werden, ohne daß der Teilnehmer diese Information einsieht und an Dritte weitergeben kann. Diese Daten sind schließlich ein handelbares Gut, für das dem Teilnehmer ein paar Pfennige in Rechnung gestellt wurden. Der Anbieter kann sich gegen Mißbrauch schützen, indem er die Daten und das erforderliche Programm zur Auswertung mit dem öffentlichen Schlüssel der Karte verschlüsselt und an diese überträgt. Nur in der geschützten Umgebung der Karte kann die Information dann installiert werden. Bei der Benutzung wird lediglich die Uhrzeit und die Vorwahl vom Telefon an die Karte übertragen – wieder ohne direkt auf den Speicher zugreifen zu können. Als Antwort sendet die Karte eine Protokolldateneinheit, die die Vorwahl des Providers enthält.

Derartige SmartCards müssen nicht notwendigerweise im Scheckkartenformat auftreten. Es gibt SmartCards im kleineren SIM-Format, das bei Mobiltelefonen eingesetzt wird oder auch als Ring (www.ibutton.com). Schließlich besteht die Möglichkeit, kontaktlos mit dem Terminal zu kommunizieren. Hierbei dient die induktive Kopplung von Karte und Lesegerät zur Datenübertragung. Dabei lassen sich Entfernungen von bis zu 1,5 Metern überbrücken. Zu beachten ist bei dieser Lösung jedoch, daß ein Angreifer „mithören“ kann. Folglich sind Daten zusätzlich zu verschlüsseln. Erste Anwendungen induktiver SmartCards finden sich bei Zugangssystemen, wie z.B. für Skilifte.

Anwendungsbereiche

- Neben der Nutzung als „elektronischer Mitgliedsausweis“ beim Skilift oder bei der Mitarbeiterkarte werden SmartCards
- für das Authentisieren (elektronische Signatur),
- für das elektronische Bezahlen (siehe Geldkarte weiter unten),
- Zur Zeiterfassung,
- als Träger persönlicher Profildaten, z.B. für Patientendaten oder bei Kunden von Online-Shops eingesetzt (siehe dazu auch den Abschnitt zum Profilmanagement).

XXX

Standards für SmartCards

Bei der Standardisierung von SmartCards lassen sich mehrere Ebenen unterscheiden, die im Laufe der Jahre vereinheitlicht wurden:

1. Auf der physikalischen Ebene wurden Abmessungen, Plazierung und Größe der Kontakte, Betriebsspannung-

gen usw. festgelegt. Diese Konventionen finden sich im Standard ISO/IEC 7816 [XXX]

2. Die nächste Ebene wird ebenfalls vom ISO/IEC 7816 definiert und bezieht sich auf Übertragungsprotokolle, Nummernsysteme, Datenrepräsentationen, Kommandos und höherwertige Konstrukte wie SCQL – Structured Card Query Language. Auch die Sicherheitsarchitektur einer SmartCard ist noch Teil dieses Standards.
3. Erst mit dem Standard der PC/SC-Arbeitsgruppe (PC SmartCard), bestehend aus Bull, Gemplus, Microsoft, IBM, Schlumberger, SNI, Sun Microsystems, Toshiba, Veriphone und anderen, werden geräteunabhängige API-Definitionen festgelegt, so daß eine Interoperabilität unterschiedlicher Karten in unterschiedlichen Betriebssystemen garantiert werden kann. Diese API-Definition bezieht sich weniger auf eine Programmierschnittstelle für Software, die in der SmartCard ausgeführt werden soll, sondern vor allem auf die Integration des SmartCard-Lesegerätes in das Betriebssystem des PCs oder der Workstation. Entsprechende Schnittstellen sind beispielsweise für Windown 98 und NT5.0 vorgesehen.
4. Nachdem nun die Integration der SmartCard in den PC sichergestellt ist, liegt der nächste Schritt in der Vereinheitlichung der Ausführungsumgebung in der SmartCard. Hier spielt *Java* eine wichtige Rolle. Nahezu alle Entwickler (Bull, Gemplus, IBM, Netscape, Sun, Schlumberger, Visa et al.) sind bestrebt, SmartCards mit einer eigenen Java Virtual Machine (JVM) zu liefern. Durch die Java-bedingte Abstraktion vom konkreten Betriebssystem und der Hardware ist eine Ebene gegeben, auf der Anwendungsentwickler unabhängig von der Technologie des Kartenherstellers programmieren können. Der von den genannten Unternehmen entwickelte Standard heißt OpenCard (www.opencard.org) und setzt auf die Spezifikation der PC/SC-Gruppe auf. Hierbei steht neben einer einheitlichen Schnittstelle der drastisch reduzierten JVM vor allem der Austausch über signierte APDU (Application Protocol Data Units) und die Definition einer High-Level-API beispielsweise für das Signieren oder Dateizugriffe im Vordergrund.

Java-SmartCards

JavaCard ist eine Version der Sprache Java für SmartCard-Betriebssysteme. Aktuell befindet sich JavaCard in der Version 2.0, die eine Java Virtual Machine (JVM) als Teil des Karten-Betriebssystems vorsieht. Damit steht eine gemeinsame, standardisierte Schnittstelle zur Ausführung von Java-Anwendungen zur Verfügung. Die Unternehmen Visa hat mit einigen anderen zur Weiterentwicklung dieses Standards das JavaCard Forum etabliert (<http://www.javacardforum.com>), während MasterCard einem anderen Konsortium angehört (<http://www.multos.com>), das mit MultOS eine weitere nicht-proprietäre Plattform entwickelt. Auch Microsoft hat einen eigenen Standard zur Programmierung von SmartCards angekündigt: Das SmartCard Software Development Kit (SCSDK).

JavaCard stellt nur eine drastisch reduzierte Ausführungsumgebung für Java-Programme zur Verfügung. Funktionen wie Multithreading, Garbage Collection oder Exceptions stehen hier nicht zur Verfügung. Ein „Cardlet“ – eine auf der SmartCard ausführbares Java-Programm – wird mit Hilfe eines Postprozessors für Java-Klassendateien erzeugt. Dabei wird ein sog. In-Card-Bytecode-Translator eingesetzt, der aus der Klassendatei eine JCBC-Datei erzeugt (JavaCard-Bytecode). Ein solcher Translator wird beispielsweise von Strategic Analysis angeboten (EZFormatter©). Die Cyberflex-Karte von GemPlus verfügt über eine eigene Virtual Machine für Java, die Cardlets aus dem JCBC-Format in die Maschinensprache der SmartCard übersetzt. Unterstützt wird die JVM vom Kartenbetriebssystem, welches das Nachrichten-Management, das Dateisystem und Security-Funktionen unterstützt.

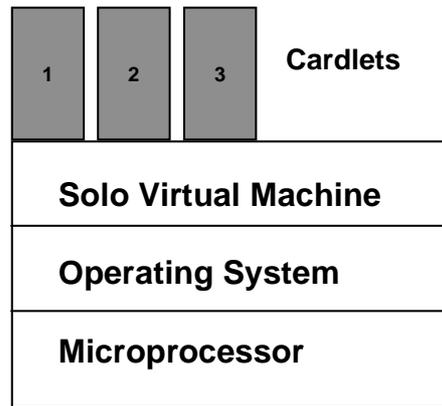


Abb. 10: Aufbau einer Java-SmartCard von GemPlus

SmartCard-Lesegeräte

In ihrer einfachsten Form sind Geldkarten-Lesegeräte bekannt, die den Ladebetrag der Karte anzeigen und für etwa 10 Euro zu kaufen sind. Dieser Preis ist realisierbar, da sie in beträchtlicher Stückzahl hergestellt werden und funktional stark reduziert sind.

Die wichtigste Entwicklung ist jedoch die Integration von Lesegeräten in den PC. Hier sind verschiedene Entwicklungen möglich:

- Integration in einen einen 3,5“-Floppy-Disk-Dummy. Bei diesem Verfahren wird eine SmartCard in eine dafür hergestellte Hülle gelegt und in den Diskettenschacht des Laufwerks geschoben. Dieser Adapter setzt die Signale des Schreib-/Lesekopfes in entsprechende Datenprotokolleinheiten der SmartCard um. Dabei erscheint die Karte dem System gegenüber wie eine normale Floppy-Disk. Vorteil dieses Verfahrens ist die Portabilität des Lesegerätes und sein geringer Preis. Fisher International Systems bietet den Disketten-Adapter Smarty rechnet bei entsprechenden Stückzahlen mit einem Endpreis von rund 40 Euro.
- Externes Lesegeräte über serielle Schnittstelle, Universal Serial Bus oder als PC-Card. Diese Lesegeräte sind in der Regel teurer (100 Euro) und belegen einen zusätzlichen Port in der Peripherie des Systems. Der Vorteil dieser Geräte liegt darin, daß PINs direkt am Gerät eingegeben werden können, so daß keine sicherheitsrelevante Information über unsichere Kanäle ausgetauscht werden. Sie sind eher als Übergangsmodell zu betrachten.
- Integration des Lesegerätes in die Tastatur. Diese Systeme erlauben eine Verschlüsselung von Daten wie beispielsweise Paßwörtern oder PINs bevor sie in das Betriebssystem des PCs übergehen. Der Tastatur-Hersteller Cherry bietet multifunktionale Kartenlesetastaturen an, die mit Preisen von unter 100 Euro bald auch für die Massennutzung durch Privatanwender erschwinglich werden.

XXX

Der Hinweis auf die notwendigen Stückzahlen verdeutlicht, daß die technischen Lösungen zwar im Vorgriff auf das Endkundengeschäft entwickelt wurden und zur Verfügung stehen, die Größenvorteile mangels einsatzfähiger Anwendungen aber noch nicht zum Tragen kommen. So konkurrieren die jetzt eingeführten elektronischen Geldbörsen, der Pay-Card von Telekom und Bundesbahn und der GeldKarte von Banken und Sparkassen, als Offline-Zahlungsmittel, doch den Emittenten und vor allem den Bankenverbänden ist es nicht gelungen, über den Einsatz an Geldautomaten und einigen Einzelhändlern hinaus den Point-of-Sale auf das Endgerät des Kunden auszudehnen. "HighTech-Industrie, LowTech-Management", bringt der Consultant und frühere Geschäftsführer der Orga Kartensysteme in Paderborn, Lutz Martiny, den Stand der Dinge kritisch auf den Punkt. Er vermißt ein Gesamtkonzept und will der Art, wie beispielsweise die GeldKarte eingeführt wurde, "nicht gerade Professionalität bescheinigen". Die Beteiligten versuchten stets aufs neue, proprietäre Systeme auf dem Markt durchzudrücken, während die Entwicklung zeige, "daß nur offene Systeme erfolgreich sein können". Martiny plädiert daher für eine "Open Chipcard Initiative" der Industrie zur Einführung offener Standards.

Siemens hat einen Fingerprint-Sensor entwickelt, der im unmittelbaren Kontakt bei der aufgelegten Fingerkuppe, ohne zwischengeschalteten Scanner oder Kamera, das Linienmuster auf taktile Weise erfaßt und daraus ein elektrisches Abbild des Fingerabdrucks erzeugt. Das Array von 256x256 kapazitiven Sensoren arbeitet mit einer Auflösung von 500 dpi. Das Erfassungsprogramm destilliert aus dem Abbild die Minutien – Linienenden, Ver-

zweigungen und Wirbel, die auch in der Kriminalistik zur zweifelsfreien Identifizierung dienen – heraus und legt sie in einer nur 1 kB großen Datei als Referenzmuster ab. Mit diesem Muster wird dann bei der Zugangsprüfung der aktuell aufgenommene Abdruck verglichen.

Ein soches System kann zusammen mit der Erkennungssoftware auf einem Laptop installiert werden. Die Authentifikation des Benutzers erfolgt dabei innerhalb einer Sekunde. Ein solches System wird beispielsweise zu Zugangssicherung für Laptops oder Mobiltelefone eingesetzt. Ein solches System kann allerdings auch in die PC-Tastatur eingebaut werden – sogar direkt in die Enter-Taste, um jede Eingabe, die mit 'Enter' abgeschlossen wird, mit einem Authentisierungscheck zu verbinden.

Eher wird die biometrische Prüfung des Fingerabdrucks wohl den lästigen und für heutige Sicherheitsanforderungen unzureichenden PIN-Schutz der Karten im Zahlungsverkehr ablösen. Gelingt es, den Sensor zusammen mit der Verarbeitungselektronik auf einer SmartCard zu integrieren, könnte die Sicherheitsprüfung auf der Karte abgewickelt werden und müßte nicht hinter dem Lesegerät oder Terminal stattfinden. Das würde die datenschutzrechtlichen Bedenken vieler Benutzer ausräumen, die selbst kontrollieren wollen, was mit ihren Daten geschieht. Erstmals in der Geschichte der Computertechnik wird damit die Speicherung und Verwaltung von persönlichen Daten unabhängig von zentralen Datenbanken und Archiven möglich. "Die Chipkarte", so Hamann, "schützt die Privatsphäre des einzelnen".

Sicherheitsfragen

SmartCards sind speziell für sicherheitssensitive Anwendungen entwickelt worden. Daher verfügen sie über entsprechende Schutzmaßnahmen auf unterschiedlichen Ebenen:

- Zugang nur über APIs
- Verwendung abhörsicherer, kryptographischer Kommunikationsprotokolle
- Festlegung eines validierten Kommunikationsmodells zwischen SmartCard und Gegenstelle
- Sicherung der SmartCard gegen physikalische Eingriffe

Der PC/SC-Standard legt einige API-Funktionen fest, mit deren Hilfe sicherheitsrelevante Mechanismen genutzt werden können. So erlaubt beispielsweise der Befehl *Verify*, Daten, die an die Karte übergeben werden, mit dort gespeicherten zu vergleichen. Diese Funktion läßt sich beispielsweise zur Verifikation von PIN-Nummern oder Paßwörtern einsetzen. Ein Fehlbedienungsähler auf der Karte ist in der Lage gescheiterte Versuche zu protokollieren, so daß ein Geheimnis nicht durch beliebiges Ausprobieren der Karte entlockt werden kann.

Der Befehl *External Authenticate* bzw. *Internal Authenticate* erlaubt eine Authentisierung der Karte durch einen Challenge-Response-Mechanismus.⁷ Dabei erhält die Karte im ersten Schritt einen Challenge-Wert vom Kommunikationspartner. Anschließend sendet die SmartCard den Response-Wert an den Partner zurück. Ist die Verifikation des Wertes erfolgreich, sendet der Partner im zweiten Schritt einen eigenen Response-Wert an die Karte zurück, um in der Karte zu prüfen, ob die Gegenstelle die Karte erkannt hat. Nun erst kann davon ausgegangen werden, daß die Karte authentisiert ist. Ein solcher Zwei-Wege-Handshake erlaubt es dem Kommunikationspartner für den Rest der Verbindung – je nach Authentisierung – auf die ganze Karte (d.h., das gesamte Dateisystem) oder auch nur auf Teile zuzugreifen.

Angreifern bieten sich bei mangelhafter Implementierung der genannten Schutzmaßnahmen Möglichkeiten Informationen auszulesen oder gar zu überschreiben. Dabei kann sich ein Hacker Softwarefehler zunutze machen, d.h. Protokollfehler, undefinierte Zustände im Betriebssystem etc. Nur durch einen beweisbar sicheren Entwurf des Betriebssystems und seiner Zustände kann dieses Angriffspotential ausgeschlossen werden.

Gleiches gilt für Teilfunktionen der SmartCard-Software. Wenn beispielsweise der Krypto-Koprozessor so naiv implementiert wird wie vor einiger Zeit die SSL-Sicherung bei Netscape (Verwendung immer wieder gleicher Zufallszahlen zur Schlüsselgenerierung), dann wird diese Funktion vorhersagbar. Neuere SmartCards verfügen zur Vermeidung derartiger Probleme über verlässliche Zufallszahlengeneratoren.

Durch physikalische Eingriffe wie Hardware-Manipulation oder Potentialdifferenzanalyse ist es in der Vergangenheit gelungen, Speicherinhalte auszulesen. Auch solchen Angriffen sind SmartCards heute gewachsen, da sie

⁷ Bei diesem Verfahren wird das Paßwort nicht im Klartext vom Client an den Server übertragen. Stattdessen sendet der Server an den Client einen Zufälligen Code (den Challenge), den der Client mit Hilfe seines Paßworts lokal verschlüsselt und an den Server überträgt. Da dieser ebenfalls über das Paßwort des Client verfügt, kann er den Client authentifizieren. Ein Anfreifer, der die Kommunikation abhört, ist nicht in der Lage, auf das Paßwort zuzugreifen.

eine Verletzung ihrer Schutzschicht „spüren“ können und in solchen Situationen ihre Funktion notfalls einstellen.

Da neuere SmartCard-Technologien mit einem hohen Sicherheitsniveau entworfen werden, sollte auch nicht mehr erwartet werden, daß ein Geheimschlüssel existiert, der für Informationen auf allen Karten einer geschlossenen Benutzergruppe einsetzbar ist (z.B. zur Verschlüsselung der PIN-Nummer).

Bei induktiven SmartCards ist besonders darauf zu achten, daß Mithörer die Karte nicht physikalisch verändern müssen. Folglich ist die Kommunikation zwischen SmartCard und Gegenstelle zusätzlich zu verschlüsseln. Das Problem liegt hier in der Stromversorgung, die über Induktionsspulen erfolgt. Häufig reicht sie nicht aus, um Protokolldateneinheiten zu verschlüsseln.

Am 22. Juni erschien in der New York Times ein Artikel über die Sicherheit von SmartCards. Anlaß war die Veröffentlichung eines Verfahrens, mit dem die geheimen Schlüssel auf SmartCards entdeckt werden können. Das Verfahren wurde bereits 1997 von Paul Kocher (Cryptography Research, San Francisco) entwickelt und basiert darauf, daß die elektrische Spannung auf aktiven Chipkarten gemessen und mittels statistischer Methoden daraus Rückschlüsse auf den geheimen Schlüssel der Chipkarte gezogen werden können. Das "Differential Power Analysis" genannte Verfahren soll auf alle gängigen SmartCards anwendbar sein. Der Aufwand zur Durchführung dieses Angriffs wird, wenn das DPA-Verfahren bekannt ist, als nicht sehr groß eingeschätzt. Allerdings setzt die Durchführung des Angriffs natürlich voraus, daß der Angreifer die SmartCard besitzt.

Aktuelle Entwicklungen

Der Markt für SmartCards expandiert zur Zeit rasant, insbesondere durch regulatorische Einflüsse wie z.B. das Signaturgesetz. Dabei ist Deutschland einer der weltweiten Standorte im Bereich der Chipkarten-Innovation: Von 1139 Patentanmeldungen in Deutschland und Europa zwischen 1990 und Ende 1997 kamen 472 aus der Bundesrepublik. Erst in großem Abstand folgen Japan (191 Patentanmeldungen), die USA (147) und Frankreich (119). Analytiker von Frost&Sullivan schätzen, daß der Weltmarkt bis zum Jahre 2003 ein Volumen von mehr als 5 Mrd. Dollar aufweisen wird, wobei auf SmartCards ein Anteil von mehr als 40% entfällt.

Entsprechend optimistisch schätzt man bei Siemens, dem Weltmarktführer für SmartCard-Chips, die Umsatzentwicklung für die nächsten Jahre auf 35% jährlich ein. Es wird erwartet, daß im Jahre 2010 zwischen 20 und 35 Milliarden Chipkarten weltweit im Umlauf sind.⁸ Auch der Markt für Karten-Chips entwickelt sich entsprechend qualitativ und quantitativ weiter. Durch die Fortschritte der Halbleitertechnik gewinnen die Systemingenieure erheblich an Design-Flexibilität; der Trend geht vom Chip-on-Card zum System-on-Card. Weil aus Gründen der mechanischen Stabilität des Siliziumträgers die maximale Grundfläche von Karten-ICs auf 25mm² beschränkt bleibt, zielen die Hersteller zur Realisierung komplexerer Funktionen bereits auf die dritte Dimension und auf Systeme, die das Chip-Layout "stapeln".

Es ist zu erwarten, daß in einigen Jahren bis zu 64 MB für das ROM zur Verfügung stehen. Damit lassen sich vollständige Workstation-Betriebssysteme mit Java Virtual Machines auf dem Niveau des heutigen Sprachstandards integrieren.

⁸ Ulrich Hamann, Leiter des Produktgebiets Chipkarten- und Sicherheits-Ics bei Siemens, auf der OmniCard 1999.

5.3 Elektronisches Bezahlen

Das elektronische Bezahlen (electronic payment) ist eines der Lieblingkinder aller EC-Buchautoren. In der Pionierphase Anfang der Neunziger galt es noch als Mysterium, Geld in elektronischer Form zu handhaben. Recht schnell entwickelten sich dann aber die ersten Prototypen wie NetCash, eCash, NetBill, CyberCash usw. Zudem gesellten sich alsbald weitere Standards und Produkte hinzu, die das neue Medium Internet zum Bezahlen mit "klassischen" Verfahren wie Scheck, Lastschrift und vor allem Kreditkarten vereinten. Irgendwann war die Aufmerksamkeit des geeigneten Beobachters für das n+1. System erschöpft, so daß Heerscharen teilweise hervorragender Diplomarbeiten [Gentz97] erforderlich waren, um die steigende Flut transparent zu machen. Heute schätzt man die Anzahl der Zahlungsverfahren auf 35 [Ricarda Weber, <http://medoc.informatik.tu-muenchen.de/Chablis/MStudy>] bis über 120 [Steve McConnell XXX?]. Klar, daß diese Welt für eine derartige Masse an Verfahren keine Integrationkraft besitzt, zumal sich viele von diesen als experimentelle Prototypen allein auf die technische Umsetzung beschränkten.

Während in den letzten Jahren noch einige recht intelligente Nachzügler wie z.B. MilliCent die Bühne am einen Ende betraten, brach am anderen bereits der Shoot-Out zwischen den Veteranen aus: FirstVirtual – technisch schlicht und schlank, dafür aber mit ansprechendem Business Modell – starb im Sommer 1998 einen fulminanten Tod. Als die Mark-Twain-Bank später schließlich eCash aufgab, fuhr ein kalter Wind durch die Fangemeinde. Auch MilliCent selbst konnte bislang noch keine Bank von seiner Profitabilität überzeugen.

Während also Micropayment-Verfahren auf der Stelle treten und sich bemühen, mit unerwartet großzügigen Serviceleistungen seitens der betreibenden Banken potentielle Händler- und Kunden zu missionieren, teilen sich Verfahren, die die Kreditkartenzahlung unterstützen, den wachsenden Markt im wesentlichen untereinander auf. Sollte man deswegen vom Glauben an Micropayment-Verfahren abfallen? Auch hier fällt eine Antwort schwer. Internet-Experten wie z.B. Esther Dyson [Dyso97] sprechen Micropayment-Verfahren eine rosige Zukunft ab. Das Hauptargument lautet etwa folgendermaßen: Für Micropayments wird häufig eine Bandbreite in der Größenordnung von Pfennigbruchteilen bis etwa 1 Euro definiert. Am unteren Ende sind diese kaum profitabel, vor allem nicht im Vergleich zu Banner-Werbung, die zudem ein sehr viel schlichteres Abrechnungsmodell zuläßt. Und am oberen Ende drohen Kreditkarten-basierte Verfahren, das Terrain der Micropayment-Systeme zu erobern: Glaubt man den Spekulationen der KK-Gemeinde, ist zu erwarten, daß aufgrund der Rationalisierungseffekte der Online-Verfahren die Transaktionskosten soweit gesenkt werden können, daß auch Beträge unterhalb eines Euro schmerzlos – d.h. für die Banken rentabel – bezahlt werden können.

Somit also von zwei Seiten eingeeengt, befinden sich Micropayment-Systeme bereits auf dem Rückzug, bevor sie überhaupt ihren Part auf der Bühne der Zahlungssysteme spielen konnten. Warum soll sich ein Finanzinstitut bzw. ein Händler neben Banner-Werbung und Kreditkarten- bzw. Lastschriftverfahren denn noch ein weiteres Verfahren – und damit einen hohen Betriebskostensockel – leisten, wenn dies nur für einen schmalen Bereich gilt. Viel besser wäre es doch, Zahlungsaktivitäten in diesem Bereich durch Einnahmen im oberen Segment der Macro-Payments (zehn bis einige hundert Euro) zu subventionieren? Neben diesen allgemeinen Gründen besteht bei individuellen Verfahren häufig das Problem der mangelnden Integration in die Macro-Payment-Infrastruktur: mindestens ist ein zusätzliches elektronisches Portemonnaie (Wallet) erforderlich (welches den Benutzer zusätzlich belästigt) oder gar das Eröffnen eines weiteren Girokontos bei der Bank, die das Micropayment-Verfahren in Umlauf bringt. Nun ist nicht jeder Kunde ein Micropayment-Fan um der Sache selbst willen, daher reagiert er im Zweifel mit Zurückhaltung.

XXX

Zahlungsgewohnheiten:

Im Gegensatz zu den USA spielen Kreditkarten in Deutschland eine untergeordnete Rolle: je 100 Einwohner existieren nur 17 Karten (insgesamt etwa 14 Mio Karten) und über 45 Millionen GeldKarten. Im Ausland ist dieses Verhältnis fast umgekehrt: in den USA besitzt ein Einwohner durchschnittlich 1,67 Karten, Großbritannien kommt auf 0,53.

Tabelle XXX: Anteile der Zahlungsarten in Prozent bezogen auf den Umsatz des Einzelhandels in Deutschland in Milliarden (1994-1997)

Zahlungsart	1994	1996	1997
Bar	78,7	76,5	76,5
Scheck	8,3	6,5	3,5
Rechnung	6,5	6,5	5,0
kartengestützt	6,2	9,9	14,5
ec-cash	0,8	2,0	2,5
EC-Lastschrift	1,7	4,0	8,0
Handelskarte	0,4	0,4	0,5
Kreditkarte	3,3	3,5	3,5
Sonstige	0,3	0,5	0,5

Nach wie vor beeindruckend ist das verschwindend geringe Volumen der Kreditkartenzahlung beim deutschen Einzelhandel. Diese Information sollte jeder Betreiber eines Online-Shops genau bedenken, wenn an deutsche Konsumenten verkauft werden soll. Im Vergleich zu den USA werden Schecks ebenfalls kaum eingesetzt.

Neben der ebenfalls in Deutschland stark dominierenden Barzahlung hat sich vor allem EC-Cash und das EC-Lastschriftverfahren durchgesetzt.

Bevor wir nun in einige Beispiele des Electronic Payment abtauchen, sei noch der dezente Hinweis angebracht, daß dieses Thema dissertationsfüllend ist und in verschiedenen Publikationen weiter vertieft wird. Dabei möchte ich natürlich weder mein Erstlingswerk [XXX Elektronische Märkte im Internet] übergehen, noch [XXX Diss, Springer]. Zugegebenermaßen gibt es jedoch noch reichlich weitere Literatur, die dieses Thema behandelt: XXX... Wenn auch etwas älter, so geben auch Furche und XXX [XXX] sowie Peter Wayner [XXX] einen brauchbaren Überblick über Verfahren, die bis vor etwa zwei Jahren noch heißgehandelt wurden.

Am wärmsten empfehlen möchte ich zu diesem Thema allerdings die Forschungsberichte des Instituts für Technikfolgenabschätzung und Systemanalyse (ITAS) der Universität Karlsruhe. Knud Böhle und Ulrich Riehm hatten dort in den Jahren 1997 und 1998 im Rahmen des Projektes „PEZ“ – Projekt Elektronische Zahlungssysteme – nicht nur eine Mailliste zu diesem Thema moderiert, sondern auch eine fast tausendköpfige Online-Community zusammengebracht, die EC-Themen wie Online-Handel, Geldkarte, SET, Micropayment-Systeme und vieles mehr in einer sachlichen und erfrischenden Form diskutierten. Als Ergebnis diese Projekts möchte ich auf daher auf den Bericht „Blütenträume – Über Zahlungssysteminnovationen und Internet-Handel in Deutschland“ verweisen, der Ende 1998 erschienen ist [BöRi98].

Im folgenden wurden einige Verfahren aus der Vielzahl von Internet-Zahlungsverfahren ausgewählt, die besonders interessant oder besonders relevant sind. Hierbei geht es nicht um eine erschöpfende Aufbereitung dieses Themas. Vielmehr sollen die Verfahren nach ihren praktischen Einsatzbereichen klassifiziert und im Hinblick auf ihre Eignung im Kontext der Internet-Ökonomie bewertet werden. Die Verfahren sind im einzelnen:

- Einfache Varianten
 - 0190er-Nummer
 - SSL-Verschlüsselung für Kreditkarten- und Lastschriftverfahren
- Kreditkartenbasiert:
 - FirstVirtual
 - CyberCash
 - SET
- Kartenbasierte Verfahren
 - GeldKarte
 - PayCard, Mondex, VisaCash ...
- E-Cash von DigiCash
- Online-Inkasso-Systeme

- T-Online-Billing
- MilliCent
- eCharge, WebBill etc.

5.3.1 Die einfachsten Varianten

Bevor wir uns die anspruchsvollen Verfahren der elektronischen Bezahlung näher ansehen, sollte festgehalten werden, daß es auch sehr viel einfacher geht, über das Internet gehandelte Produkte abzurechnen.

Ruf' an!

Man nehme eine Telefonkarte, rufe eine 0190er-Nummer des Händlers an und lasse sich für einen genügend langen Zeitraum von dessen Werbung berieseln. Wenn nach X Sekunden der Preis erreicht ist – sagen wir 2 Euro – wird von der Voice-Box noch kurz ein individueller Code mit 20 Zeichen durchgegeben. Für ein paar Sekunden und Groschen mehr kann man sich diesen noch einmal wiederholen lassen, bis man sich endgültig sicher ist. Dann setzt man diesen Schlüssel ein, wenn es darum geht, sich schlüpfrige Fotos, Videoclips oder Online-Chats zu Gemüte zu führen. Nach einem Monat verfällt der Schlüssel und das Spiel beginnt wieder von vorne. Dieser Mechanismus ist simpel für alle Beteiligten. Anonymität ist wählbar: Man kann per ISDN von zuhause oder von der Telefonzelle aus anrufen. Das einzige Problem liegt in den horrenden Transaktionskosten: die Telekom zweigt 50%(!) der Umsätze für sich ab. Allerdings liegen auch 0190er-Nummern bereits auf dem Opfertisch des Ex-Monopolisten (XXX Ja??), so daß hier Aussicht auf Entspannung besteht.

Die Moral der Geschichte lautet etwa wie folgt: Während der Akademiker noch über die 25. Zusatzfunktionalität des bei Verlust wiederherstellbaren, Micropayment-fähigen Multiwährungs-Wallet für anonyme Zahlungen mit Double-Spending-Detection forscht, dreht sich das Rad der Geschichte rastlos weiter und löst dieses Problem auf denkbar einfache Weise. Unter der Annahme, daß zukünftig für 0190er-Nummern vielleicht nur noch 10-20% vom Provider verlangt werden, besteht für Micropayment-Verfahren auch noch im mittleren Bereich eine weitere Bedrohung. Warten wir es ab - es bleibt spannend!

Kreditkartenzahlung und Verschlüsselung mit SSL

Man stelle sich folgende Situation vor: eine universitäre Gruppe, die sich mit der Technologie der wesentlichen elektronischen Zahlungsverfahren auskennt, brennt darauf, ein entsprechendes Verfahren für die von ihr veranstaltete ECommerce-Konferenz (TREC'98, <http://vsys-www.informatik.uni-hamburg.de/trec98>) einzusetzen. In Erwägung gezogen wurden E-Cash, SET, CyberCash, X-PAY, FirstVirtual, Electronic Cash. Keines dieser Verfahren ließ sich binnen weniger Monate einsetzen: Entweder war das Verfahren nicht international anerkannt (die Teilnehmer mußten sich von überall her registrieren können) oder organisatorische bzw. finanzielle Einschränkungen verhinderten eine rasche Registrierung als „Merchant“. Darüber hinaus waren einige der Verfahren entgegen dem Marketinggetöse zum gegebenen Zeitpunkt noch in keiner Weise einsatzbereit. Schließlich war es ein Kunststück, bei den Banken einen Mitarbeiter ans Telefon zu bekommen, der überhaupt „E-Cash“ von „Electronic Cash“ unterscheiden konnte.

Die Folge dieses „Reality Checks“ war Kreditkartenzahlung über HTML-Formulare und SSL als Standard-Verschlüsselungsmechanismus. Da hierbei nur die Übertragung der Daten vertraulich erfolgt, jedoch nicht ihre serverseitige Verarbeitung, mußten wir uns daher selbst um technische und organisatorische Datenschutzmaßnahmen kümmern.

SSL erlaubt eine authentifizierte, vertrauliche Kommunikation durch Erweiterung des allen Internet-Protokollen zugrundeliegenden TCP/IP-Protokolls. Unabhängig von der Anwendung werden hier alle Nachrichten pauschal verschlüsselt. Zu erkennen ist dies an dem Namen der jeweiligen Web-Seite, der mit <https://> beginnt.

Die Erzeugung eines Schlüsselpaares kann beispielsweise bei SSL nach dem Diffie-Hellman-Protokoll erfolgen. Soll RSA als Verfahren verwendet werden (so daß auch die Authentizität des Servers anhand eines Zertifikats verifiziert werden kann), so ist bei einer Zertifizierungsautorität ein öffentlicher Schlüssel registrieren und zertifizieren zu lassen. Wir taten dies in Verbindung mit Thawte, einer Südafrikanischen CA und prompt erhielten wir bzw. der Leiter unserer Arbeitsgruppe einen Anruf seitens der CA, bei dem anhand einiger sehr spezifischer Fragen die Identität von Person und Organisation sichergestellt werden konnte.⁹

⁹ Für Puristen ist dieses Verfahren noch lange nicht ausreichend, da trotz allem nicht beweisbar sichergestellt werden kann,

Nahezu alle Online-Anbieter setzen heute SSL in Verbindung mit Kreditkartenzahlungen ein. Dabei ist jedoch weder händlerseitiger noch käuferseitiger Betrug ausgeschlossen. Um dies zu erreichen, müssen sich Verfahren wie z.B. CyberCash (Vermeidung von Betrug durch den Händler) oder SET (Vermeidung von Betrug auf beiden Seiten) durchsetzen.

Für den tatsächlichen Inkasso-Prozeß ist noch eine Kooperation mit einem sog. Acquirer, d.h. einer Organisation, die die Zahlungsaufforderung entgegennimmt und den Geldtransfer zwischen den Bankkonten von Kunde und Händler initiiert, erforderlich. Als Acquirer diente im Falle der Konferenz die GZS (Gesellschaft für Zahlungssysteme), an die wir über ein beauftragtes Inkassounternehmen die Zahlungsinformationen weiterleiteten.

Die Rolle des Acquirers kann aber auch die Bank des Händlers übernehmen, die den Betrag von der Kreditkartengesellschaft bzw. von der kartenausgebenden Bank einfordert. Anders gesagt, die Bank des Händlers fordert eine bestimmte Geldsumme im Namen des Kreditkartenkunden für eine bestimmte bestellte Ware ein. Es gibt vor allem in den USA ähnliche Konstellationen, in denen die Einziehung der Beträge für den Händler von einer Bank oder einem anderen Dienstleister vorgenommen wird. In Deutschland ist das aber eher unüblich: Der Händler kann direkt von einem Serviceunternehmen (B+S oder GZS) oder Kreditkartenunternehmen (Diners oder AmEx) die Beträge gutgeschrieben bekommen. Somit ist zumindest in Deutschland die akquirierende Bank nicht die Bank des Händlers.

Zu beachten ist im übrigen bei SSL-verschlüsselter Kommunikation, daß nicht nur das Formular zur Eingabe der Zahlungsinformation verschlüsselt übertragen werden sollte, sondern vor allem die Übertragung der Daten an den Händler. Im Rahmen unserer Online-Registrierung für die Konferenz, hatten wir zunächst nur die Übertragung der Daten verschlüsselt, was beim Ausfüllen des Formulars noch nicht zur Anzeige des SSL-Logos (z.B. vollständiger Schlüssel bei Netscape) führte. Erst nachdem der Käufer den „Send“-Knopf gedrückt hatte, wurde die Übertragung verschlüsselt. Psychologisch ist dieser Ansatz schlecht, da zum Zeitpunkt der Dateneingabe nicht das Gefühl vermittelt wird, daß eine sichere Übertragung vorliegt. Aus diesem Grunde wurde nach einigen Anfragen der Teilnehmer bereits das Formular verschlüsselt. Umgekehrt ist jedoch ein viel schwerwiegenderes Problem gegeben: Wenn sich der Kunde im Gefühl wiegt, ein sicher übertragenes Formular auszufüllen, kann es dennoch passieren, daß die Übertragung an den Server unverschlüsselt erfolgt, nämlich, wenn im HTML-Dokument für den „Send-Button“ nicht folgendes zu erkennen ist:

```
<FORM METHOD=POST ACTION=https://www.irgendeinshop.de>
```

Vermutlich hat sich noch kein Online-Kunde damit beschäftigt, sich den Quellcode des Formulars anzusehen...

5.3.2 Lastschriftverfahren

Für einen Händler, dessen Geschäft durch langjährigen Betrieb eine angemessene Bonität als Unternehmen erworben hat, besteht die Möglichkeit, per Lastschriftverfahren Geldbeträge direkt vom Konto des Kunden abzubuchen. Dieses Verfahren kann im Prinzip ähnlich wie bei der Kreditkartenzahlung eingesetzt werden, indem eine Autorisierung des Händlers erfolgt, den betreffenden Geldbetrag abzubuchen. Im normalen Geschäftsbetrieb ist hierzu jedoch (im Gegensatz zur Kreditkartenzahlung) eine schriftliche Einwilligung des Kunden erforderlich.

Aus diesem Grunde wird das LSV beim Online-Kauf in der Regel nicht direkt zwischen Händler und Kunde eingesetzt, sondern indirekt über Dritte, die im Auftrage des Händlers die Abbuchung vornehmen. Ein Beispiel für eine solche Lösung ist das EDD-Verfahren von CyberCash (siehe auch weiter unten), bei dem der Server der CyberCash GmbH einen sog. DTA-Satz erstellt (Datenträgeraustausch). Dieses standardisierte Format wird in Deutschland für die Übermittlung von Zahlungsaufträgen eingesetzt. Beim EDD liefert das CyberCash-Gateway eine Benachrichtigung an den Händler, so daß dieser seine Ware an den Kunden ausliefern kann. Der DTA-Satz wird anschließend an die Bank des Händlers übermittelt und der Kunde erhält eine Bestätigung der Zahlungstransaktion. Eine EDD-Zahlung dauert ca. 15 Sekunden [Dres98, Schu98].

Tabelle XXX: Transaktionsgebühren bei EDD

	Umsatz je Transaktion von - bis	Entgelt in v.H. des Umsatzes
DM	10,00 - 14,99	4
DM	15,00 - 19,99	3

daß das beantragte Zertifikat sich wirklich auf einen öffentlichen Schlüssel bezieht, der mit dem geheimen der Universität korrespondiert.

DM	20,00 - 24,99	2,75
DM	25,00 - 29,99	2,5
DM	30,00 - 49,99	2,0
DM	50,00 - 69,99	1,75
DM	70,00 - 99,99	1,5
DM	ab 100,00	1

Zur Zeit wird daran gearbeitet, das Schriftformerfordernis bei der Einwilligung zum LSV durch einen elektronischen Vertrag zu ersetzen. Mit Hilfe des Signaturgesetzes besteht hier die Möglichkeit, eine Gleichstellung der elektronischen Signatur zu bewirken und somit das Zustandekommen einer Einwilligung auf elektronischen Wege zu fördern. Es ist zu erwarten, daß seitens der Banken ein erhebliches Interesse an der raschen Gleichstellung besteht. Dieses Interesse wird gestützt durch die heutige Verfügbarkeit von Software wie CyberCash's edd.

Weitere pragmatische Lösungen

www.sperrmüll.de ist ein Online-Katalog mit Kleinanzeigen. Dieser Katalog kann nach Belieben online und ohne Gebühren durchstöbert werden. Der Katalog enthält jedoch nur Produkt- und keine Anbieterinformationen. Hat der Interessent ein Angebot gefunden, muß er sich über eine 0190er-Nummer zum Preis von 1,21 DM/Minute die Telefonnummer des Anbieters besorgen. Auch hier liegen die Transaktionskosten durch die Telekom bei 50%.

Das klassische Bezahlen über das SWIFT-Netz

Wenn wir heute eine internationale Überweisung durchführen, erfolgt dies über das SWIFT-Netz. SWIFT (Society for Worldwide Interbank Financial Telecommunication) ist eine von Banken betriebene Kooperation, die den weltweiten, sicheren Datenaustausch zwischen über 6.000 Finanzinstituten in 174 Staaten realisiert. Davon sind nur ca. 3.000 Banken, die anderen setzen sich zusammen aus Börsenmaklern, Investmentgesellschaften, Fondsverwaltern, Börsen etc. Im Jahre 1997 wurden über das SWIFT-Netz über 800 Millionen Nachrichten ausgetauscht, dabei belief sich das durchschnittliche tägliche Volumen auf über 2 Trillionen US-Dollar!

XXX

5.3.3 Kreditkartenbasierte Verfahren

Ein großer Anteil der heute genutzten Internet-Zahlungsmethoden basiert auf Kreditkarten. Dies liegt zum einen an der hohen Durchdringung, zum anderen an der einfachen Übertragbarkeit von KK-Zahlungen auf das Internet. Heute sind in Deutschland ca. 14 Millionen, in den USA über 460 Millionen und weltweit etwa 1 Milliarde Karten im Umlauf.

Während im SSL-Beispiel weiter oben die Nutzung von Kreditkarteninformation als verschlüsselte Daten nur eine von beliebig vielen Anwendungen ist, sind die im folgenden dargestellten Verfahren spezialisiert in der Weise, daß eine dedizierte Organisation bzw. Softwarekomponente zur Verarbeitung der Zahlungsinformation eingesetzt wird.

Im folgenden wollen wir die Verfahren von FirstVirtual (aus „historischen Gründen“), CyberCash und SET untersuchen. Dabei sollte man folgenden Frage im Hinterkopf behalten: Wie wird das Vertrauen der beteiligten Akteure erhalten – organisatorisch, technisch oder durch eine Kombination der beiden Ansätze?

5.3.3.1 FirstVirtual

FirstVirtual wurde 1994 gegründet, 4000 Händler, 240.000 Kunden in 166 Ländern. FirstVirtual ist das System der 1994 gegründeten FirstVirtual Holding Company, USA. Das verblüffend einfache Konzept war eines der ersten, die tatsächlich funktionierten und angewendet wurden (seit Oktober 1994). Es basiert im wesentlichen auf der Übertragung einfacher e-Mail-Nachrichten, was nicht weiter verwunderlich ist, wenn man sieht, daß zu sei-

nen Erfindern beispielsweise Nathaniel Borenstein und Einar Stefferud gehören (Stefferud war der erste, der 1975 eine Mailing-List im Internet schuf. Borenstein war einer der Mitentwickler des MIME-Mail-Standards). Während seiner erfolgreichsten Phase umfaßte FirstVirtual mehr als 4000 Händler und 240.000 Kunden in 166 Ländern. Bis Mitte 1998 blieben davon nur 2000 Händler und über aktive 60.000 Kunden bei FirstVirtual. Am 20. Juli 1998 gab das Unternehmen bekannt, daß es sich aus dem Markt für Zahlungssysteme zurückzieht und sich in Zukunft ganz auf sichere Nachrichtenübertragung konzentriert. Den Kunden wurde eine Migration zu CyberCash angeboten. FirstVirtual wird hier dennoch kurz beschrieben, da es zum einen zu den erfolgreichsten Produkten im Bereich der Internet-Zahlung zählt, und zum anderen ist es durch seine elegante Schlichtheit und seinen frühen Einsatz von „historischem“ Interesse ist.

Funktionsweise

Ein potentieller Käufer eröffnet ein Konto bei FirstVirtual. Dies kann er per e-Mail, Telnet oder über das WWW. Dabei teilt er FirstVirtual seinen Namen, seine Adresse, ein Kennwort und eine e-Mail-Adresse mit, unter der er erreichbar ist. An diese e-Mail-Adresse sendet FirstVirtual eine Bestätigung und eine gebührenfreie Telefonnummer, über die der Käufer dann seine Kreditkartennummer (z.Zt. Visa oder Mastercard) an FirstVirtual bekanntgibt.

Die Kreditkartennummer wird also nicht über das Internet übertragen, sondern über das vergleichsweise sichere Telefonnetz. Der Anbieter muß ebenfalls ein Konto bei FirstVirtual eröffnen. Dabei gibt es zwei Modelle, eins eher für kleinere Anbieter, das andere für größere Firmen. Will ein Käufer etwas von einem Anbieter erwerben, so gibt er diesem seine FirstVirtual-Kontonummer. Der Anbieter sendet diese zusammen mit seiner eigenen Kontonummer, dem zu zahlenden Betrag und einer Beschreibung des Handelsgutes an FirstVirtual. FirstVirtual wiederum sendet eine e-Mail an die Adresse, die zu der eingeschickten Kontonummer des Käufers gespeichert ist.

Der Käufer kann dann auf die e-Mail auf eine von drei möglichen Arten antworten: YES, um zu signalisieren, daß der Kauf tatsächlich von ihm ausgegangen ist und vollzogen werden soll. NO, um anzuzeigen, daß er seine Meinung geändert hat und vom Kauf zurücktritt (FirstVirtual behält sich vor, Käufer, bei denen dieses Verhalten häufiger auftritt, vom System auszuschließen.) Die letzte mögliche Antwort ist FRAUD, was bedeutet, daß der Käufer diesen Kauf nie initiiert hat. In diesem Fall wird FirstVirtual keine Zahlung vornehmen und den Vorfall näher untersuchen, beispielsweise um festzustellen, ob möglicherweise der Anbieter derjenige ist, der versucht hat, hier einen Betrug zu begehen.

Bestätigt der Käufer den Kauf, belastet FirstVirtual seine Kreditkarte mit dem angegebenen Betrag, schickt dem Anbieter eine Bestätigung der Bezahlung und überweist das Geld nach Abzug der Gebühren auf das Konto des Anbieters (mit unterschiedlich langen Verzögerungsfristen, um sicherzustellen, daß die Kreditkarte auch tatsächlich gedeckt ist).

Technische Voraussetzungen

Die technischen Voraussetzungen sind im Falle von FirstVirtual denkbar gering. Anbieter wie Käufer benötigen im Prinzip jeweils nur einen e-Mail-Anschluß. Natürlich ist es wünschenswert, daß der Anbieter über eine geeignete Plattform wie beispielsweise einen Web-Server verfügt, um seine angebotenen Handelsgüter darstellen zu können. Auf Käuferseite ist dann ein geeigneter Mechanismus erforderlich (also beispielsweise ein Web-Browser), um sich einen Überblick über das Angebot zu verschaffen.

Von FirstVirtual selber wird sogar ein eigener Server zur Verfügung gestellt (FirstVirtual InfoHaus, <http://www.infohaus.com>), über den interessierte Anbieter Daten an ihre Kunden verkaufen können. Für die Speicherung der Daten und die Abwicklung der Transaktionen fallen zusätzliche Gebühren an, aber für Anbieter, die neu in diesem Marktbereich sind, ist das sicherlich eine interessante Möglichkeit.

Organisatorische Voraussetzungen

Bei FirstVirtual muß der Anbieter ein Konto bei einer amerikanischen Bank haben. Genauer gesagt, muß die Bank das „United States Automated Clearing House (US ACH) System“ unterstützen. Eine Liste solcher Banken war zum Zeitpunkt unserer Recherche nicht verfügbar. Die einzige Auskunft auf FirstVirtuals Website bezüglich nicht-amerikanischer Banken war, daß einige kanadische Banken dieses System unterstützen wollen.

Deutsche Ableger amerikanischer Banken kommen laut der FirstVirtual-Website auch nicht in Frage, da diese das „US ACH“ auch nicht unterstützen. Die Filiale, bei der das Konto geführt wird, muß ihren Sitz physikalisch

in den Vereinigten Staaten haben.

Kosten

Auf Käuferseite beschränken sich die Kosten auf eine jährliche Gebühr von US\$ 10,—. Bei den Anbietern wird unterschieden zwischen Pioneer-Sellern und Express-Sellern. Express-Seller können nur solche Anbieter werden, die bereits auf herkömmliche Art und Weise Kreditkarten abgerechnet haben, somit bei den Kreditkarten-Firmen bekannt sind und ihre Vertrauenswürdigkeit unter Beweis gestellt haben. Pioneer-Seller zahlen nur eine jährliche Gebühr von US\$ 10,—, Express-Seller hingegen eine Anmeldegebühr von US\$ 350,— sowie in den Folgejahren jährlich US\$ 250,— zur Verlängerung ihres Vertrages mit FirstVirtual. Dafür erhalten Express-Seller ihre Gelder von FirstVirtual in einer Frist zwischen 4 und 23 Tagen, Pioneer-Seller hingegen müssen zwischen 91 und 108 Tagen auf ihr Geld warten. Die jeweils längeren Fristen ergeben sich aus Akkumulationsphasen, in denen geringe Beträge möglichst angesammelt werden sollen, um geringe Zahlungen nicht mit allzuhohen Gebühren zu belasten.

Beide Anbieter bezahlen je Transaktion, also je Zahlung eines Kunden an einen Anbieter, 2% des zu zahlenden Betrages + US\$ 0,29 an FirstVirtual. Darüber hinaus fallen pro Überweisung von FirstVirtual an einen Anbieter US\$ 1,— Überweisungsgebühren an. Um den Anteil dieser Überweisungsgebühren an den zu transferierenden Geldern möglichst gering zu halten, wird versucht, in den oben bereits erwähnten Akkumulationsphasen mehrere kleine Zahlungen zusammenzufassen.

Bewertung

Die größte Stärke von FirstVirtual lag zweifelsohne in seiner Einfachheit. Die technischen Voraussetzungen waren sowohl beim Händler als auch beim Endkunden denkbar gering. Zahlungstransaktionen wurden einfach über e-Mail erledigt. Da so gut wie jeder, der im Internet aktiv ist, über einen eigenen e-Mail-Account verfügt, waren die technischen Voraussetzungen somit von jedermann ohne weiteres zu erfüllen. Auch war das System relativ sicher, da keine sensiblen Daten wie Kreditkartennummern über das Internet übertragen wurden. Aus diesem Grund konnte auf aufwendige Verschlüsselungsmechanismen gänzlich verzichtet werden. Vertrauen wurde somit ausschließlich mit Hilfe organisatorischer Mittel geschaffen. Ein Kunde brauchte sich nicht zu fragen, ob sensitive Daten wirklich verschlüsselt werden, wenn er der Betreiberorganisation FirstVirtual traute.

Als nachteilig erwies sich die Beschränkung auf Händlerseite auf den amerikanischen Markt (genauer gesagt die Notwendigkeit eines amerikanischen Bankkontos). Die Tatsache, daß es FirstVirtual trotz eines relativ großen Händlernetzes mit ca. 2000 an das System angeschlossenen Händlern nicht geschafft hat, wirtschaftlich zu arbeiten und letztlich diesen Teil seines Geschäftsfeldes aufgeben mußte, läßt befürchten, daß auch anderen Anbietern von Zahlungssystemen, die zumeist über wesentlich weniger Händler verfügen, harte Zeiten bevorstehen werden.

5.3.3.2 CyberCash

CyberCash ist ein Zahlungssystem, das verschiedene Zahlungsmittel (Kreditkarten, digitale Münzen und Lastschriften) in eine einheitliche Software integriert. Über den eigenen Verschlüsselungsmechanismus hinaus hat CyberCash angekündigt, auch den SET-Standard für kreditkartenbasierende Zahlungen in sein System zu integrieren.

Funktionsweise

Zur Bezahlung mit CyberCash muß sich der Kunde zuerst eine „Wallet“ genannte Software von der Website CyberCashes (www.cybercash.de), von einer Bank oder von der des Händlers auf den eigenen Computer laden. Anschließend sind in einem Setup-Prozeß seine Kreditkartendaten zu nennen. Dann kann die Wallet für Einkäufe benutzt werden.

Für den Händler ist die Registrierung bei CyberCash ähnlich einfach. Auch er benötigt eine Software, die mit der Software des Kunden sowie dem CyberCash-Server den Zahlungsvorgang abwickelt. Zur Verschlüsselung der Daten nach dem CyberCash-proprietären Verfahren wird SSL eingesetzt. Darüber hinaus wird das SET-System (s.u.) in die CyberCash-Software mitintegriert, so daß Verschlüsselung und Zertifizierung in Zukunft nach dem SET-Standard erfolgen dürfte.

Für den Kauf eines Produktes per Kreditkarte löst der Kunde mit einem in die WWW-Seiten des Händlers integrierten „Pay“-Button den Zahlungsvorgang aus. Von der CyberCash-Software des Händlers erhält das Wallet daraufhin sämtliche Orderdaten. Das Wallet wird automatisch aktiviert und öffnet ein Fenster, in dem der Kunde nun sein Zahlungsinstrument auswählt und die Zahlung bestätigt. Der Kunde gibt bei der Installation des Wallets seine Kreditkarteninformationen ein, die daraufhin verschlüsselt abgelegt werden und bei weiteren Transaktionen abrufbar sind. Diese Daten werden mit dem RSA-Verfahren (1024-bit Schlüssel) für den CyberCash Gateway-Server verschlüsselt und an den Händler gesendet. Damit kann der Händler nicht auf die Zahlungsinformation zugreifen (vgl. Abb. XXX).

Der Händler fügt seine elektronische Signatur hinzu, ohne die Daten des Kunden einsehen zu können. Die „CashRegister“ genannte Software des Händlers nimmt die Daten entgegen, fügt ihnen die Signatur des Händlers hinzu und sendet sie an den CyberCash-Server. Dieser dekodiert die Daten und verifiziert die enthaltenen Kreditkarten-Informationen mit dem entsprechenden Kartenunternehmen. Fällt diese Überprüfung positiv aus, wird das Kreditkartenkonto des Kunden belastet und eine entsprechende Bestätigung an den Händler zurückgeschickt. Dieser kann dann den Versand der Ware veranlassen oder dem Kunden online den Zugriff auf bestimmte Daten oder eine Download-Möglichkeit, z.B. für Software, zur Verfügung stellen. Eine Verifikation der Bestellung zwischen CyberCash-Server und der Wallet-Software des Kunden findet nicht statt. Sämtliche Schritte werden dabei automatisch ausgeführt, so daß der gesamte Vorgang etwa 20-30 Sekunden dauert.

Neben der Bezahlung mit Kreditkarte sieht CyberCash auch den Einsatz von sogenannten CyberCoins vor. Diese dienen für sogenannte „Micropayments“, also als Zahlungsmittel für Beträge zwischen US\$ 0,25 und US\$ 10,—, bei denen die Abrechnung per Kreditkarte wegen der dabei anfallenden Gebühren nicht lohnend wäre. Technisch gesehen handelt es sich bei diesen CyberCoins allerdings nicht um echte digitale Münzen, sondern eher um ein Transaktionssystem, bei dem ein Käufer ein Konto bei einer Bank anlegt, dieses mit einem gewissen Betrag füllt und es mit Hilfe seiner Wallet verwaltet. Die Zahlungstransaktionen verlaufen analog zum Verfahren beim Einsatz von Kreditkarten.

Schließlich unterstützt CyberCash das in Deutschland recht attraktive Lastschriftverfahren. Hierbei wird ein Händler, der nach dem Lastschriftverfahren Abbuchungen von Kundenkonten durchführen darf, vom Kunden dazu autorisiert.

Technische Voraussetzungen

Die technischen Anforderungen der CyberCash-Software sind eher gering. Die Wallet-Software für den Endkunden liegt in Versionen für Windows sowie für Macintosh-PCs vor (für Macintosh bislang allerdings ohne CyberCoin-Integration), die CashRegister-Software für Händler in Versionen für Windows NT sowie für diverse Unix-Implementationen (darunter Solaris, HP/UX, AIX und sogar Linux).

Organisatorische Voraussetzungen

Ende des Jahres 1997 waren nur amerikanische Kreditkarten zur Teilnahme an diesem Verfahren zugelassen. 1998 startete ein Feldtest in Deutschland, bei dem jeder teilnehmen konnte, der sich die Wallet-Software installierte und seine Konto- und Kreditkartendaten mitteilte. Betrieben wird der Feldtest von der CyberCash GmbH, der Dresdner Bank, Sachsen LB, West LB und einigen weiteren. Zu beachten ist jedoch, daß die Einrichtung eines Kunden Ende 1998 noch mehrere Tage dauerte. D.h. ein spontaner Kauf konnte nicht durchgeführt werden, auch wenn allgemein akzeptierte Kreditkarten zur Zahlung verwendet werden sollten. Auch hier kommt das Henne-Ei-Problem wieder zum Tragen: Wenn nicht in ausreichendem Umfang Wallet-Software zur Verfügung steht (z.B. durch Bündelung mit Web-Browsern), werden Händler kaum Kunden finden, die per CyberCash bezahlen wollen. Vorteilhaft für die Verbreitung von CyberCash ist die häufig anzutreffende Bündelung mit Händler-Software, wie z.B. mit Intershop.

Auf der amerikanischen WebSite von CyberCash wurden im Dezember 1998 ca. 500 Händler aufgeführt, die CyberCash als Zahlungsmittel akzeptieren [XXX cc-im]. Auf der deutschen Website von CyberCash wurden im Dezember 1998 nur 20 Händler genannt, die an Pilotprojekten teilnahmen [XXX cc-dm].

Kosten

Während CyberCash selber Ende 1997 noch auf seiner Website angab, daß weder für den Käufer noch für den Anbieter Gebühren erhoben werden (da CyberCash die Abwicklung mit den Kreditkarten-Anbietern abrechne),

so hat sich dieses Preismodell mittlerweile geändert. Eine Möglichkeit ist, daß der Händler die Abrechnung mit dem Kreditunternehmen vornimmt, von dem er CyberCash bezogen hat. Sollte er seine Abrechnung direkt mit CyberCash vornehmen, so muß er in den USA pro Transaktion mit einer Gebühr von US\$ 0,20 bis US\$ 0,60 rechnen (evtl. zuzüglich einer monatlichen Gebühr) [XXX cc-kg].

Diese Gebühren würden Zahlungen im Micropayment-Bereich natürlich ad absurdum führen. So ist für den Einsatz von CyberCoin auch ein anderes Preismodell vorgesehen: Pro stattgefunderer Transaktion US\$ 0,10 plus 4 % des zu zahlenden Betrages [XXX cc-cg]. Beim kleinstmöglichen Betrag beim Einsatz von CyberCoin (US\$ 0,25) wären dies Gebühren in Höhe von US\$ 0,11, also stattliche 44%!

In Deutschland gelten seit Sommer 1998 für CyberCoin und EDD die in Tabelle XXX und XXX angeführten Gebühren:

Tabelle XXX: Transaktionsgebühren bei CyberCoin

	Umsatz je Transaktion von - bis	Entgelt in v.H. des Umsatzes
DM	0,05-0,19	30
DM	0,20-0,29	25
DM	0,30-0,49	20
DM	0,50-0,74	15
DM	0,75-0,99	10
DM	1,00-1,24	8
DM	1,25-1,49	7
DM	1,50-2,99	6
DM	3,00-4,99	5
DM	5,00-9,99	4
DM	10,00-50,00	3
Kassen- abschluß:		1,--

Das Mindestentgelt liegt bei CyberCoin bei monatlich DM 20,--.

Bewertung

CyberCash versucht, mit seiner Wallet-Software ein ganzes Portfolio an Zahlungsmitteln anzubieten. Dieser Ansatz ist grundsätzlich sehr interessant, denn so wie sich bei den konventionellen Zahlungsmitteln unterschiedliche Arten von Transaktionen etabliert haben (Bezahlung mit Bargeld, Lastschriften, Kreditkarten, Überweisungen, Lastschriften etc.), so erweisen sich auch im Internet unterschiedliche Zahlungsmechanismen als sinnvoll. Bislang besteht das System allerdings ausschließlich aus der Abrechnungskomponente für Kreditkarten. Der münzbasierte Teil läuft bislang nur in Pilotprojekten, und die dabei für den Händler anfallenden Gebühren sind gerade bei kleineren Beträgen exorbitant hoch. Auch die Abrechnung mit Lastschriften wird bislang nur in Pilotprojekten realisiert.

Die Integration der Abrechnung nach dem SET-Standard in die CyberCash-Wallet ist sicher eine interessante Entwicklung, aber solange CyberCash dieses Verfahren nicht durch eigene, proprietäre Zahlungsarten wie Münzen oder Lastschriften sinnvoll ergänzt, stellt sich die Frage, weshalb Kunden und Händler nicht gleich SET einsetzen sollten. Für unseren Einsatzzweck war CyberCash leider wegen der damals erforderlichen US-Kreditkarte auf Seiten des Käufers nicht geeignet. Sämtliche Kooperationen mit deutschen Banken befanden sich noch im Pilotstatus.

Anzumerken ist ferner, daß sich in der Praxis viele Anbieter jedoch für die Nutzung eines Java-Wallets entscheiden, damit ein Kunde nicht von seinem spontanen Kaufentschluß abgehalten wird. Heute bietet die Firma Brokat (zusammen mit TeleCash) mit X-Pay eine Software an, die ebenfalls – analog zu Cybercash – die drei Verfahren Kreditkarte, Lastschrifteinzug und TC-Moneybytes unterstützen.

Cybercash ist (neben X-Pay und SET) eines der wenigen gängigen Systeme, die einem Betrug durch den Händler vorbeugen. Laut Kriminalitätsstatistiken [XXX FBI] liegt das höchst Betrugsvolumen gerade beim Betrug durch

Händler. Wird zusätzlich noch verhindert, daß der Kunde mit einer gestohlenen Kreditkarte einkauft, kann die nächste Betrugsmöglichkeit verhindert werden. Dies kann CyberCash jedoch nicht leisten. Aus diesem Grunde wartet alle Welt auf den breiten Einsatz von Systemen, die Zertifikate zur Authentisierung des Kunden verwenden. Das Protokoll SET (Secure Electronic Transaction) hilft, diese Lücke in Form eines standardisierten Protokolls zu schließen.

5.3.3.3 SET

SET ist ein weiteres Zahlungsprotokoll zur Übermittlung von Kreditkartennummern über das Internet. Es befindet sich seit 1997 bei einigen Informationsanbietern (z.B. My-World von Karstadt) in der Einführungsphase.

SET wurde gemeinsam entwickelt von einem Konsortium, bestehend aus Visa, Mastercard und einigen IT-Herstellern. Der SET-Standard arbeitet auf der Basis eines asymmetrischen Public-Key-Verfahrens mit digitalen Zertifikaten. Er garantiert so die Authentizität der Marktteilnehmer sowie die Bezahlung und Auslieferung der bestellten Waren. SET ist ein Protokoll, welches allen Teilnehmern (Käufer, Verkäufer, Bank) Informationen über die beteiligten Individuen, den Kaufpreis und Kaufgegenstand sowie Details der Bezahlung zukommen läßt. Lediglich die Kreditkartendaten bleiben dem *Verkäufer* verborgen. Dies wurde explizit beim Entwurf des Protokolls gefordert. Wenn diese Gefahrenquelle erfolgreich vermieden werden kann, ist zu erwarten, daß sich die kriminalitätsbedingten Transaktionskosten erheblich reduzieren und damit auch die gesamten Transaktionskosten, die von der Kreditkartenbenutzung herrühren.

An einer SET-Transaktion sind die folgenden Rollen beteiligt:

- Cardholder als Kunde,
- Händler bzw. Verkäufer, bei dem der SET Merchant Server installiert ist,
- Kartenherausgeber (Issuer). Diese Bank (o.a. Finanzdienstleister) hat den Kunden mit einer Kreditkarte ausgestattet. Der Herausgeber sichert dem Händler bei der Autorisierung zu, daß der zu zahlende Betrag zur Verfügung steht.
- Der Acquirer verarbeitet Zahlungen im Auftrage und für den den Händler. Er erhält die Autorisierung dazu vom Herausgeber.
- Payment Gateway. Diese spezifische SET-Software dient dem Acquirer zur Kommunikation mit dem Händler.
- Zertifizierungsautorität. Hier werden Zertifikate für Kunde, Händler und Payment Gateway vergeben und verwaltet.

Protokoll

Die SET-Infrastruktur besteht aus drei Bestandteilen: das *Elektronische Portemonnaie* (SET-Wallet), welches sich auf dem Rechner des Benutzers befindet, ein *SET-Server*, der auf dem Web-Server des Händlers installiert ist und dem *SET Payment Server* (auch Payment Gateway) seitens der Bank des Verkäufers.

Um das SET-System zu benutzen, muß der Käufer zunächst die Kreditkartennummer in das Wallet eingeben. Die meisten Implementierungen speichern dabei diese Nummer verschlüsselt auf der Festplatte oder in einer Smart-Card. Erst durch Eingabe des Benutzerpasswortes gegenüber dem Wallet kann dieses die Kreditkartennummer verarbeiten. Damit können beliebig viele Benutzer einen einzelnen PC als "SET-Terminal" teilen. Ferner wird ein Schlüsselpaar generiert.

Wenn der Kunde eine Bezahlung veranlaßt, wird die Zahlungsinformation verschlüsselt an den Verkäufer gesendet und von diesem unterschrieben an seine Bank weitergeleitet. Dort erfolgt die Entschlüsselung sowie die Verifikation der Unterschrift. Im positiven Fall veranlaßt die Bank den Zahlungstransfer. Abschließend wird eine Quittungs-Nachricht an Verkäufer und Käufer zurückgesandt. Ebenso wie bei CyberCash schützt das SET-Protokoll die Kreditkartendaten vor der Einsichtnahme durch den Verkäufer. Dadurch wird das höchste Angriffspotential seitens des Verkäufers (welches erfahrungsgemäß in der realen Welt gegeben ist) vermieden.

SET ist hinsichtlich der Vertraulichkeit beschränkt auf die Übertragung der Kreditkarten-Nummer. Eine weitreichende Unterstützung hätte die Exportmöglichkeiten von SET-Software erheblich eingeschränkt, da RSA als Verfahren eingesetzt wird.

SET unterscheidet zwischen Informationen, die nur dem Käufer und Verkäufer bekannt sind (die bestellten Pro-

dukte bzw. *Order Information, OI*), und solchen, die nur Käufer und Bank teilen (*Kreditkartennummer* bzw. *Payment Information, PI*).

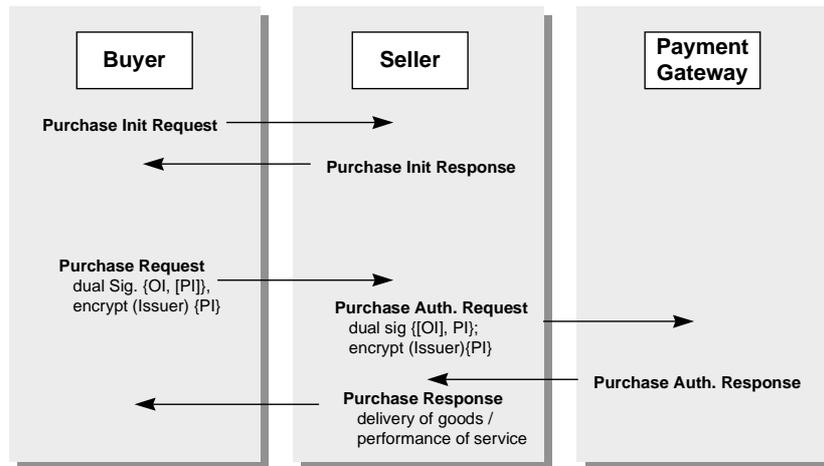


Abb. 11: Nachrichtenfluß bei SET

Bei der Autorisierung gibt es verschiedene Zahlungsvarianten, die vom Händler gewählt werden können und die auch bei der herkömmlichen Kreditkartenzahlung vorzufinden sind: Entweder wird nur eine Autorisierung der Zahlung durch den Acquirer vom Herausgeber eingeholt (Authorize Now and Capture Later). In diesem Fall findet noch keine Buchung statt. Diese könnte einmal monatlich oder am Ende des Tages zwischen den Finanzinstituten durchgeführt werden. Im anderen Fall (Authorize and Capture Now) wird der Zahlungsbetrag sofort dem Konto des Händlers gutgeschrieben (wenn er beispielsweise ein Soft-Good sofort und unwiederbringlich liefern muß). Eine weitere übliche Variante ist „Installment or Recurring Use“. Hier werden Daten für Abschlags- oder periodische Zahlungen festgelegt. Der Acquirer ist dann autorisiert, regelmäßig einen Zahlungsbetrag über den Herausgeber beim Kunden abbuchen zu lassen.

“Dual Signature“

Mit Hilfe eines “Dual Signature“ genannten Verfahrens werden diese unterschiedlichen Informationen der OI und der PI mit einander in Verbindung gebracht: eine SET “Purchase Request Message“ besteht aus zwei Komponenten - eine für den Verkäufer und eine für die Bank. Die erste wird verschlüsselt mit dem öffentlichen Schlüssel des Verkäufers und die zweite mit dem der Bank.

Zusätzlich werden Hash-Werte für beide Komponenten erzeugt und aneinander gehängt. Die elektronische Unterschrift der Dual Signature wird schließlich geleistet, indem für die beiden Hash-Werte wiederum ein weiterer erzeugt und mit dem geheimen Schlüssel des Käufers unterschrieben wird.

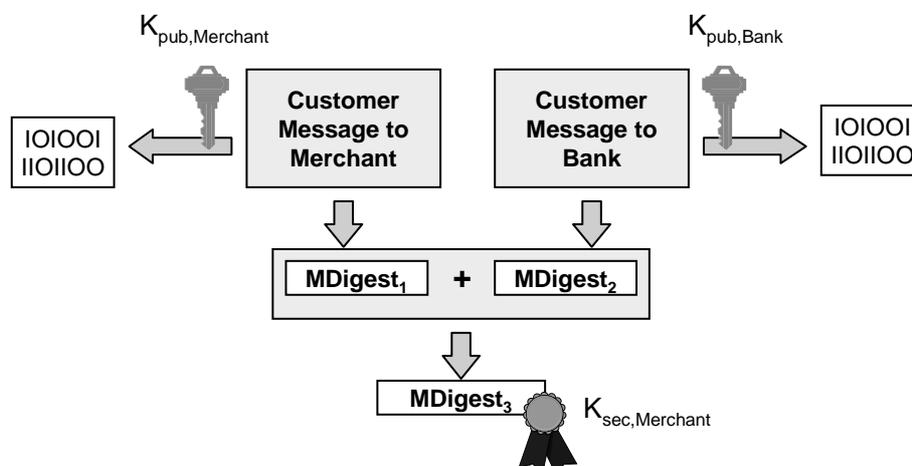


Abb. 12: Das Dual Signature-Verfahren von SET

In einigen Fällen ist es (wg. Legacy-Systemen) erforderlich, die Software des Verkäufers doch mit der Kreditkartenummer zu versehen. Dies erfolgt indirekt und optional über die Nachricht, die nach der Buchung von der Bank an den Verkäufer zurückgesendet wird.

Zertifikate

SET erfordert für die Authentisierung der beteiligten Parteien die Einbindung einer Zertifizierungsautorität (Z.B: VeriSign, TC TrustCenter, etc.). Bei dieser sind sowohl Käufer als auch Verkäufer und Payment Gateway registriert. Vor und während des Zahlungsprotokolls werden diese Zertifikate ausgetauscht, so daß je Verifikation eine weitere Kommunikation mit der Zertifizierungsautorität erforderlich ist.

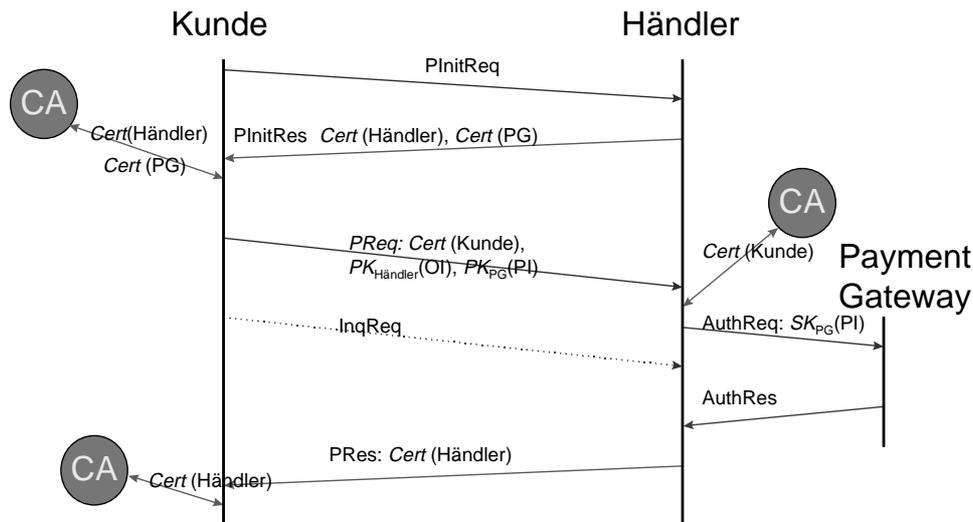


Abb. 13: Austausch von Zertifikaten beim SET-Protokoll

Im Gegensatz zu Standard-X.500-Zertifikaten besitzen SET-Zertifikate Zusatzinformationen („Extension-Attribute“), die speziell im Kontext dieses Verfahrens von Bedeutung sind. Die Unterscheidung bei SET in Zertifikate für Cardholder, Merchant und Payment-Gateway wird durch eines dieser Attribute festgelegt. Ein anderes legt fest, ob dieses Zertifikat für einen öffentlichen Schlüssel verwendet werden soll, mit dem verschlüsselte Nachrichten an den Besitzer gesendet werden sollen oder für einen (anderen!) öffentlichen Schlüssel, mit dem signierte Nachrichten des Senders verifiziert werden können (bei SET können tatsächlich für beide Zwecke unterschiedliche Schlüssel verwendet werden, obwohl dies nicht nötig wäre).

Organisatorische Voraussetzungen

Um eine einheitliche und weite Verbreitung des neuen Standards zu gewährleisten, haben die Kreditkartengesellschaften Mastercard und VISA mit der SETCo (<http://www.setco.org>) eine Zertifizierungs-Instanz gegründet. Um SET-Software in Umlauf zu bringen, muß ein Anbieter diese von der SETCo zertifizieren lassen. Die SETCo ist das Standardisierungsgremium, welches den Funktionsumfang sowie die Protokolle und Schnittstellen zwischen SET-Komponenten festlegt. Dabei bezieht sich die Zertifizierung auf einen Kompatibilitätstest des Wallets, der Händler-Software sowie des Payment-Gateways.

Einige bereits zertifizierte Produkte, z.B. von GlobeSet, Data Design, Terisa, Trintech und Verifone haben als erste das begehrte SET-Compliance-Zertifikat erhalten.

Weitere Infos:

<http://www.setco.org/matrix.html>

Auswahl SET-Anbieter: <http://www.globeset.com/products.shtml>

Interessant: SET eignet sich auch für SmartCard-Lösungen. Dieses wurde unter dem Namen C-SET bereits in Frankreich erprobt. Dabei werden sowohl Zertifikate als auch die Verschlüsselungstechnik auf der Karte unter-

gebracht. Der Vorteil liegt darin, daß nicht mehr alle Transaktionen online autorisiert werden müssen. Dadurch lassen sich Kosten sparen und evtl. Transaktionen unterhalb einer DM noch abwickeln.

Software für SET-Wallets wird inzwischen von diversen Herstellern angeboten:

- X-PAY Java Credit Wallet. Dieses SET-Wallet steht als Applet zur Verfügung und kann unmittelbar beim Kaufvorgang über das Internet geladen werden. Dieses Wallet ist ein Container für unterschiedliche Zahlungsmethoden konfiguriert worden (SET, Micropayments, Edd, normale Kreditkartenzahlung) www.brokat.de.
- CyberCash Internet Wallet. Dies ist das übliche CyberCash-Wallet (CyberCash, Edd, CyberCoin), das mit einer SET-Komponente erweitert wurde (www.cybercash.de)
- GlobeSet Wallet. GlobeSet war einer der ersten Hersteller, dessen vollständiges Sortiment an SET-Komponenten (Wallet, Merchant Server, Payment Gateway) von der SetCo zertifiziert wurde (www.globeset.com).
- IBM Consumer Wallet. Das Wallet von IBM steht als Browser-Plug-In zur Verfügung (www.ibm.com/commerce/software/payment/wallet.html).
- Microsoft Wallet. Das MS Wallet kann kostenlos geladen werden von www.microsoft.com/wallet/default.asp. Es ist ebenfalls Bestandteil neuerer Versionen von MS Windows.

Erweiterungen von SET

Die heutige Version 1.0 des SET-Standards sieht auf der Kundenseite ein installierbares Wallet vor sowie ein Zertifikat, das über das Netz von der CA erhalten wurde. Der Signaturschlüssel des Kunden befindet sich in einer verschlüsselten Datei auf der Festplatte. Zukünftige Versionen bieten Erweiterungen, die sich auf die Verwendung von SmartCards abstützen, so daß der dort generierte Signaturschlüssel verwendet werden kann. Dies erhöht das Sicherheitsniveau drastisch und erlaubt die Verwendung öffentlicher PC-Terminals, in die die persönliche SmartCard eingeführt wird. Ferner sind Erweiterungen geplant, die die Verwendung von PINs erlauben, damit sich ein Kunde gegenüber seiner Karte authentifizieren kann. Außerdem lassen sich durch diese Maßnahme Electronic Cash-Transaktionen durchführen, die in Europa neben Kreditkarten als Zahlungsverfahren vorherrschen.

Bewertung SET

SET stellt zur Zeit das einzige praktisch relevante Internet-Zahlungsverfahren mit dem größten Nutzungspotential und einer realistischen Sicherheitspolitik dar. Zur Zeit befindet es sich in Deutschland jedoch noch in der Erprobungsphase – nur wenige Anbieter nutzen SET, da auf der Kundenseite keine Nutzung der Zertifizierungsinfrastruktur erwartet werden kann. In den USA setzt sich SET zur Zeit als Ablösung der dort üblichen “klassischen“ Kreditkartennutzung durch (d.h. ohne Verschlüsselung oder mit Verschlüsselung zwischen Kunde und Verkäufer, z.B: durch SSL).

Ein weiteres aktuelles Problem ist bei SET die notwendige Zertifizierungsinfrastruktur. Kunde und Händler müssen sich bei einer Zertifizierungsautorität (CA) mit Kreditkarte sowie weiteren Daten registrieren, um ein Zertifikat zu erhalten, welches für die Verarbeitung mit SET erforderlich ist. Solange weite Kundenkreise diese Zertifizierung noch nicht vorgenommen haben, kann SET nicht oder nur mit gewissem Risiko zum Einsatz kommen. Hier ist jedoch zu erwarten, daß Banken (bzw. Verbände) an der automatischen Zertifizierung ihrer Kunden sowie an der Errichtung der erforderlichen Infrastruktur arbeiten.

Man kann grundsätzlich davon ausgehen, daß mittelfristig durch die Einführung von SET die SSL-Transaktionskosten sinken werden und damit auch das Fixum von heute ca. 0,5 DM für Kreditkartentransaktionen. Somit werden sich Kreditkarten grundsätzlich auch für Transaktionsvolumina im mittleren Bereich von DM 5,- bis DM 50 besser eignen.

Grundsätzlich problematisch erscheint die ausschließliche Nutzung von kreditkartenbasierten Verfahren speziell in Deutschland, da ein großer Teil der Bevölkerung lediglich über EC-Karten bzw. die Geldkarte verfügt. Hier bietet sich eine Erweiterung von SET an, die speziell für den deutschen Markt entwickelt wurde:

5.3.3.4 Zusammenfassung: Kreditkartenbasierte Methoden

Electronic Commerce findet idealerweise weltweit statt, daher muß auch die zugrundeliegende Zahlungsmethode weltweit zur Verfügung stehen. Dies ist heute nur bei Kreditkarten der Fall. Diese Präsenz betrifft dabei nicht nur die technische Zahlungsabwicklung, sondern vor allem auch den organisatorisch-juristischen Rahmen: üblicherweise besteht gegenüber dem Händler und dem Kartenbesitzer eine Zahlungsgarantie durch die Kartenorganisation oder den Acquirer. Diese Garantie wird auf Basis eines privatrechtlichen Vertrags gewährleistet, so daß keine gesetzliche Regulierung erforderlich ist (und vor allem keine internationale). Eine solche Infrastruktur ist bereits für den traditionellen Handel gegeben, so daß für den elektronischen keine substantiellen organisatorischen Anpassungen erforderlich sind.

XXX stimmt das so???

Letztlich kann auch bei KK-Zahlungsmethoden die Unterscheidung in „Billig-Ökonomie“ (SSL oder gar unverschlüsselte Übertragung) und „Vollkasko-Gesellschaft“ (SET) vorgenommen werden: Einen Online-Shop einzurichten, ist in der Vollkasko-Gesellschaft mit Beschaffungs- und Einrichtungskosten der SET-Software verbunden, mit der Erlangung eines Händlerzertifikates, gleichzeitig kann nur mit zertifizierten Kunden Handel getrieben werden und die „Transaktionskosten“ des Downloads eines schwergewichtigen Wallets sind zu tragen. Der SSL-Shop erfordert lediglich das Händler-Zertifikat, welches ihn generell als Teilnehmer, nicht jedoch als spezifischen SET-Händler charakterisiert. Letzteres bietet jedoch einen Nachweis, daß der Händler eine vertragliche Beziehung zu einer Kartengesellschaft eingegangen ist. Der Trade-off heißt also hier: *Sicherheit vs. Flexibilität*.

Während bei der SSL-Variante nur ein Händler-Zertifikat erforderlich ist, können dies im Extremfall bei SET sogar vier sein:

- Ein Zertifikat entspricht dem des Händlers zur herkömmlichen SSL-Sicherung der Kommunikation;
- das nächste ist erforderlich, um seinen SET-Händlerstatus nachzuweisen.
- Ein Drittes Zertifikat ist nötig, um den Kunden zu authentisieren (der ja möglicherweise mit seiner SigG-konformen SmartCard am PC sitzt) und
- schließlich kann noch die Software selbst zertifiziert sein, wie es bereits heute bei der Zahlungssoftware von Brokat der Fall ist. Hier geht es darum, Code zu authentisieren und seine Integrität zu sichern.

5.3.4 Guthabekarten

5.3.4.1 Geldkarte

Die Geldkarte ist das in Deutschland wohl prominenteste Projekt zur elektronischen Bezahlung. Es handelt sich hierbei um eine SmartCard, die mit einem Geldbetrag von bis zu 400,- DM an speziellen Terminals aufgeladen werden kann. Jede Zahlungstransaktion reduziert daraufhin einen internen Zähler auf der SmartCard. Mit der Geldkarte verfügt der Halter somit über einen vorausbezahlten Betrag, der über Händlerterminals und deren Lesegeräte beim Kauf abgebucht werden kann. Das Konzept der GeldKarte ist vom ZKA (Zentralen Kreditausschuß) entwickelt worden. Zur Zeit befinden sich über 45 Millionen Geldkarten im Umlauf. Die Geldkarte kann noch nicht über das Internet eingesetzt werden, dies liegt weniger an der Technologie (es sind natürlich Lesegeräte erforderlich), sondern vielmehr an der restriktiven Freigabepolitik des ZKA, der trotz des großen Interesses seitens der Industrie bislang keine Internet-Freigabe erteilt.

Das Zahlungsprotokoll

Eine Bezahlung mit der Geldkarte involviert etliche beteiligte Mitspieler, so daß diese zunächst einzuführen sind:

- Der *Karteninhaber* bzw. Kunde setzt die Karte ein, um entweder am Ladeterminale Bargeld auf die Karte zu laden oder beim Händler davon einen Betrag wieder abbuchen zu lassen.
- Die *Bank des Kunden* richtet für diesen zusätzlich zum Girokonto ein Verrechnungskonto ein, auf dem der Ladebetrag sowie die Kartenumsätze verbucht werden. Außerdem verwaltet die Kundenbank ein Gebührenkonto, auf dem die Provision gebucht wird, die anfällt, wenn der Kunde eine Bezahlung durchführt.

- Der *Händler* nimmt die Zahlung über sein Händlerterminal entgegen. Er muß sich selbst mit einer Händlerkarte gegenüber das Terminal authentisieren.
- Die *Bank des Händlers* ist nur beteiligt, wenn Zahlungen auf das Händlerkonto durchgeführt werden.
- Das *Ladeterminal* muß nicht notwendigerweise bei der Bank des Kunden benutzt werden, daher ist ggf. der Betreiber des Ladeterminals als ein weiterer Mitspieler beteiligt.
- Schließlich stellt die *Börsenevidenzzentrale* eine Schaltstelle dar, über die alle Zahlungstransaktionen gebucht und verfolgt werden.

Denkbar sind noch weitere Rollen wie z.B. die des Kartenherstellers oder die Datensammelstelle, über die Daten beim Laden oder Kauf weitergeleitet werden. Für unser Grundmuster einer Geldkartentransaktion sind diese Rollen jedoch irrelevant.

Im Kern werden zwei Aktivitäten unterschieden: Das *Aufladen* und das *Bezahlen*. Beim Aufladen bucht der Karteninhaber vom Girokonto einen Geldbetrag auf die Karte. Sowohl der dortige Zähler als auch das interne Verrechnungskonto werden entsprechend angepaßt. Die Information des Ladebetrags wird zusätzlich an die Börsenevidenzzentrale geleitet, wo ein weiteres Konto (das Schattenkonto) für jede in Umlauf befindliche Geldkarte geführt wird.

Das Bezahlen erfolgt durch Einführen der Karte in das Händlerterminal. Dazu muß der Kunde eine PIN eingeben, durch die die Karte bei Verlust vor Mißbrauch geschützt ist. Der am Terminal eingegebene Zahlungsbetrag wird daraufhin bestätigt. Im Anschluß meldet das Händlerterminal über das Netz des Terminalbetreibers den Betrag an die Börsenevidenzzentrale. Diese reduziert den Saldo des Schattenkontos der Karte und bucht den Betrag vom Verrechnungskonto des Kunden auf das Konto des Händlers bei seiner Bank abzüglich der Provision, die der Händler an die kartenherausgebende Bank abzuführen hat. Die Börsenevidenzzentrale kann dem Händlerterminal ebenfalls melden, ob eine Karte als verloren gemeldet wurde. Nur bei Freigabe der Zahlung wird schließlich der Betrag auf der Karte gebucht.

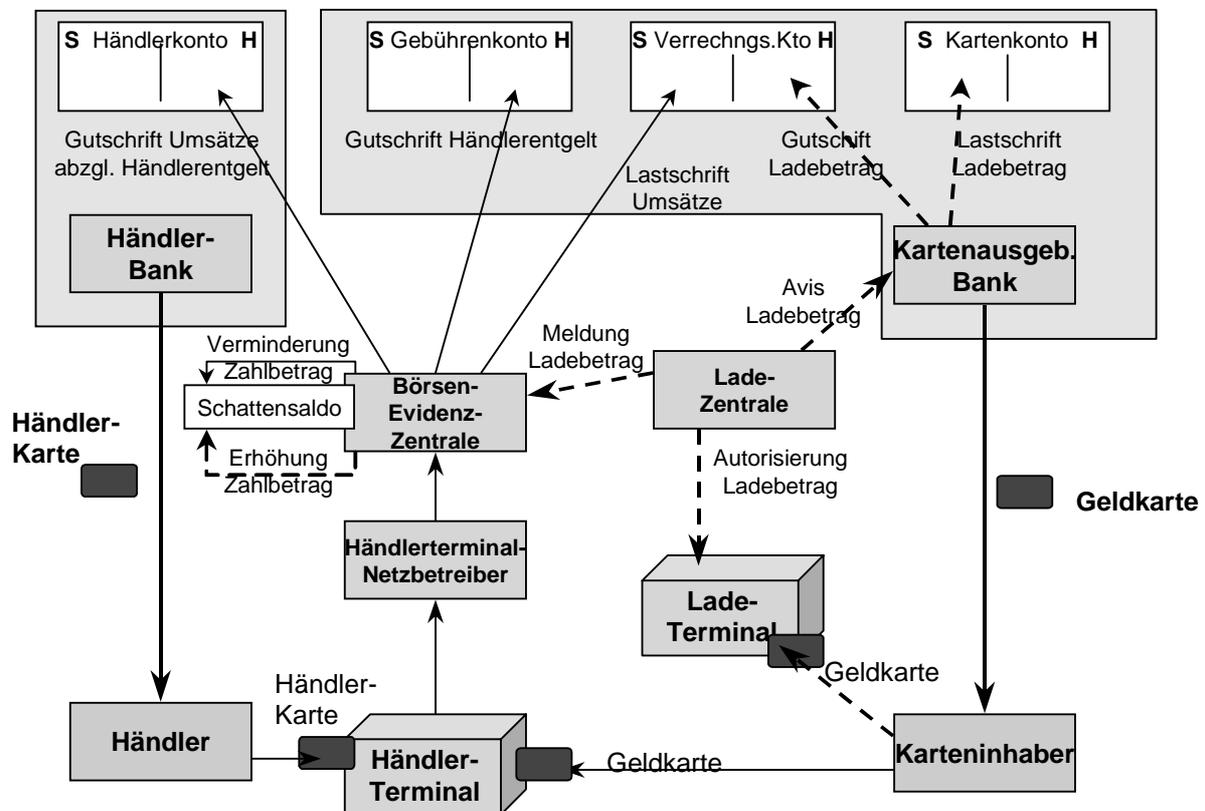


Abb. 14: Abläufe und Instanzen bei GeldKarten-Transaktionen

Datenschutz vs. Verbraucherschutz

An der Beteiligung der Börsenevidenzzentrale ist zu erkennen, daß eine zentrale Instanz über Information aller Geldkartentransaktionen in Deutschland verfügt. Da dies aus Datenschutzgründen höchst bedenklich ist, dürfen diese Daten nicht ohne weiteres an Dritte weitergegeben werden. Nur in Fällen von Kartenverlust oder Inkonsistenzen können Informationen über Transaktionen und Saldo einzelner Karten an die ausgebende Bank übermittelt werden. Somit ist es prinzipiell möglich, beim Kartenverlust die Karte zu sperren und den Saldobetrag durch die Bank zu ersetzen.

Besonders interessant (und für den Kunden relevant) kann am Beispiel der Geldkarte gezeigt werden, in welchem Zielkonflikt Datenschutz und Verbraucherschutz stehen: Ohne Evidenzzentrale wäre die Wiederherstellung des Kundenkontos nicht möglich, wenn es zu Buchungsfehlern oder Kartendefekten kommt. Diese Möglichkeit stärkt das Vertrauen des Kunden in die Zuverlässigkeit des Systems, so daß er sich als Verbraucher in einer besseren Position befindet. Andererseits würde ohne Evidenzzentrale keine Möglichkeit bestehen, über den gesamten Transaktionsdatenbestand des Geldkartenumlaufs zu verfügen. Die dort abgelegte Information ist besonders attraktiv für Marktanalysen sowie zur Erstellung von Kunden- und Händlerprofilen, so daß besondere Sicherungsmaßnahmen erforderlich sind.

Grundsätzlich kann die Information der Evidenzzentrale natürlich für alle denkbaren Beweissituationen eingesetzt werden, z.B. um einen Täter zu überführen oder als Alibi-Funktion für einen Unschuldigen. Hier liegt ein äußerst sensibler Bereich vor, bei dem die genaue Rechtslage wahrscheinlich noch nicht genau geklärt ist.

Der Bundesbeauftragte für den Datenschutz, Joachim Jacob, warnte folglich im XXX 1998 die Bürger vor aufladbaren Geldkarten, da ihre Anonymität nicht gewährleistet ist. Kritisiert wurde vor allem, daß die Kreditwirtschaft ihre Kunden nicht darüber informiert, daß sie beim Bezahlen Datenspuren legen (Zeitpunkt und Ort des Kaufs sowie der ausgegebene Betrag). Die Evidenzzentrale speichert diese Information über mehrere Jahre. XXX Quelle finden!!! Auf Knopfdruck können für jedem Kartennutzer exakte Verhaltens- und Kaufprofile erstellt werden. Auch Bundeskriminalamt und Polizei nutzen diese Informationen bereits.

White Cards

Eine Chance zur Erhöhung des Datenschutzniveaus liegt in der Herausgabe sog. WhiteCards (bzw. kontenunabhängige Geldkarten): Dies sind anonyme Geldkarten, die nicht mit einem Kundenkonto in Verbindung stehen – folglich sind sie auch nicht über eine PIN individualisiert. Aus diesem Grunde sind Ladeterminals erforderlich, mit deren Hilfe Bargeld in Form von Banknoten auf die Karte transferiert wird. Eine solche White Card ist damit anonym, wenn auch ein Bewegungs- und Transaktionsprofil für die betreffende Karten-ID erstellt werden kann.

Die entscheidende Frage ist allerdings in der Praxis, wie man als Kunde eine White Card erhält. In der Mailliste EZI-L [XXX] wurde 1998 ein nettes Beispiel gegeben, wie in der Praxis mit Anonymität umgegangen wird: Als Kunde wollte der Autor eine White Card bei seiner Sparkasse erwerben. Dies war nach etwas Aufklärungsarbeit des Leiters der Kundenbetreuung dann auch möglich: für einen Kaufbetrag von 5 DM wurde die Karte ausgehändigt. Der Haken lag jedoch darin, daß der Kunde dabei eine Überweisung des Betrags mit Angabe der White-Card-Nummer (!) unterschreiben mußte. Sicherlich lernen die beteiligten Personen seitens der Banken in Zukunft, Begriffe wie „Anonymität“, „Datenschutz“ und „Verbraucherschutz“ korrekt zu interpretieren. Dieses Beispiel zeigt jedoch, daß noch sehr viel Weiterbildungsbedarf besteht.

Besonders paranoide Menschen müßten folglich regelmäßig ihr Bargeld-Ladeterminal wechseln, hin- und wieder eine andere WhiteCard einsetzen – und dies idealerweise im Tausch mit anderen WhiteCard-Besitzern – um wirklich sicher zu gehen...

Das „Business Model“ der Geldkarte

Wer verdient eigentlich wieviel an und mit der Geldkarte? Gleich vorweg: Dies ist noch nicht geklärt, insbesondere ob sie wirklich für alle Parteien einen wirtschaftlicheren Umgang bei der Handhabung von Bargeld bietet. Folgendes Zahlenmaterial soll helfen, den Nebel etwas zu lichten:

1. Händler zahlen Provision an den Kartenherausgeber. Dies sind 0,3% des Kartenumsatzes, mindestens aber 0,02 DM.
2. Kunden zahlen Provision, wenn sie ihre Karte bei einem anderen Terminalbetreiber als ihrem Herausgeber

aufladen (bis zu 7 DM als Fixum!). Ferner wird eine Ausgabegebühr bei WhiteCards erhoben.

3. Da das Geldkartenbargeld eigentlich Buchgeld ist – es wird ja auf dem Konto der Bank geführt – kann diese es gegen Zinszahlungen an Dritte verleihen. Damit tritt folgender Effekt ein: der Zinsgewinn, den die Bundesbank mit dem im Umlauf befindlichen Bargeld erzielt (die sog. *Seignorage*), wird teilweise an die Banken abgetreten, da die Nachfrage nach Bargeld im Gegensatz zum Buchgeld abnehmen wird. In seiner Arbeit hat Wolfgang Gentz diesen Effekt sehr detailliert ausgeführt [Gentz97].
4. Der Händler „verdient“ durch einen effizienteren Umgang mit Geld an der Kasse: die Herausgabe von zuviel Wechselgeld wird vermieden und auch der manuelle Umgang mit Bargeld wird vereinfacht. Ferner wird das Diebstahlrisiko vermindert, da sich in der Kasse weniger Geldnoten befinden. Der Händler trägt allerdings auch die Provision, die an die Herausgeberbank zu zahlen ist.
5. Ähnliches gilt letztlich auch für den Kunden.

Es scheinen also alle an der Geldkarte zu verdienen.

Die Geldkarte in der Praxis

Trotz der 45 Millionen Exemplare ist die Evidenzzentrale noch nicht allzusehr ausgelastet: Im Oktober 1997 existierten nur 35.000 Händlerterminals. Dies ist recht wenig im Vergleich zu den 162.600 Akzeptanzstellen für Electronic Cash (Stand: 1Q98): 260.000 für die Eurocard und 310.000 für Visa. Bei den über 400.000 Einzelhandelsunternehmen in Deutschland (Filialen nicht mitgezählt) ist dies eine Durchdringung von weniger als 10%.

Nur 2% aller Geldkarten sind WhiteCards. Dies hängt im wesentlichen von den Herausgebern ab, da in der Bevölkerung noch nicht genügend Bewußtsein über die genauen Eigenschaften der Geldkarte besteht.

Ab Herbst 1999 sollen GeldKarten auch für öffentliche Telefone eingesetzt werden. Die Händlerkarte ist dabei in das Gerät fest eingebaut. Insgesamt würde dies etwas 100.000 öffentliche Telefone betreffen.

Desweiteren wird sich mittelfristig entscheiden, wie die deutsche Geldkarten-Lösung mit anderen im EU-Ausland harmonisiert werden kann. Dies betrifft zum einen die Unterstützung des Euro, zum anderen die internationale Interoperabilität.

Für das Jahr 2000 ist die sog. Geldkarte Typ 1 geplant, deren Basiswährung der Euro sein wird und die inkrementelle Abbuchungen unterstützen soll (wie z.B. bei zeitbezogenen Gebühren erforderlich). Damit könnte die Geldkarte sogar die Telefonkarte ersetzen.

Grundsätzlich kann die Geldkarte für mehr als nur Barzahlungen eingesetzt werden: Sie erlaubt es auch, Rabattsysteme von Händlern zu unterstützen oder Anwendungen wie elektronische Fahrscheine, Telefonkarten oder Guthabensysteme individueller Händler. So wird die Geldkarte an der Universität Trier zur Bezahlung von Dienstleistungen der Universität eingesetzt. Diese Anwendungen liegen außerhalb der Geldkartenfunktionalität, da hier der Buchungsmechanismus der Börsenevidenzzentrale nicht eingesetzt wird. In anderen Städten (z.B. Hannover) kann man die Geldkarte zur Bezahlung von Parkscheinen in Parkhäusern einsetzen.

In Eichstätt wurde ein regional begrenztes CityCard-Projekt durchgeführt, welches das Bonusmarkensystem des Handels mit der GeldKarte verbindet. Bei 13.000 Einwohnern in Eichstätt und 115.000 im Einzugsgebiet wurden 9.500 CityCards ausgegeben sowie 3.500 Kundenkarten der Banken. 8.500 Kartenbesitzer hatten auf diese Weise für 161.000 DM Bonuspunkte gesammelt. Allerdings wurden nur sieben Prozent der eigentlichen Kauftransaktionen mit der GeldKarte durchgeführt. Dieses Ergebnis ist eher enttäuschend.

Richtig interessant wird der Einsatz der Geldkarte jedoch erst im Internet, da mit ihr ein Mechanismus langfristig zur Verfügung stehen könnte, mit dem auch die beliebten Mikrotransaktionen durchgeführt werden können. Erforderlich sind jedoch im wesentlichen zwei Bedingungen: erstens muß der ZKA die Nutzung der Karte im Internet zulassen (die technische Realisierung wurde bereits 1997 demonstriert) und zweitens müssen Internet-Benutzer mit einem Kartenleser ausgestattet sein. Dieser kostet heute jedoch zwischen etwa 10 und über 1.000 Euro, je nachdem, welche Funktionen unterstützt werden (Anzeige des Betrags, Abbuchen eines Betrags, Funktionen des Händlerterminals etc.).

Die Zulassung vom ZKA setzt die Möglichkeit voraus, daß der Kunde über einen vertrauenswürdigen Kartenleser verfügt, der neben dem Zahlungsbetrag auch ein Händlerzertifikat verifiziert und anzeigt. Obwohl dies kein technisches Problem darstellt, verzögert sich die Zulassung der GeldKarte nach wie vor, da die Spezifikation für solche Zertifikate noch fehlt.

Die Deutsche Bahn AG will ihre 250.000 Mitarbeiter mit Ausweisen ausstatten, die den Geldkarten-Chip tragen. Damit besteht die Möglichkeit, nicht nur Zugangskontrollen mit der Geldkarte durchzuführen, sondern – wie an

der Uni Trier – auch interne Dienstleistungen (z.B. Bahnkantine) zu verbuchen.

Da die Geldkarte beim konventionellen Kauf am Kiosk mit dem Bargeld konkurriert, wird sie sich hier nur langfristig durchsetzen können. Industrie und Verbraucher fordern jedoch ein Zahlungsmittel, das sich auch im Internet flexibel einsetzen läßt. Eine begehrte Lösung ist hierbei die Geldkarte. Da im Internet jedoch die Software des Händlers so einfach einsehbar ist wie das Lesegerät am Kiosk, werden zusätzliche Sicherheitsmaßnahmen gefordert:

- Auf der Kundenseite muß sichergestellt sein, das der tatsächliche Zahlungsbetrag angezeigt wird und diese Funktion nicht beeinträchtigt werden kann.
- Ähnlich der Nutzung von Zertifikaten beim SET-Protokoll ist die Authentizität des Händlers sicherzustellen
- Schließlich muß sichergestellt werden, daß der Datenaustausch zuverlässig und gegen mögliche Angreifer gesichert durchgeführt werden kann.

Auch für die Bezahlung an Automaten besteht immenses Potential für die Geldkarte: In Deutschland sind 1,9 Millionen Automaten aufgestellt, die jährlich 11 Milliarden Euro Umsatz generieren. Hier können Probleme des Bargeld-Handling vermieden werden, das heute beträchtlichen Aufwand verursacht: Allein durch die Zigarettensautomaten fallen täglich(!) 46 Tonnen Münzen an. Dadurch, daß Automatenzahlungen in der Regel Micropayments sind (zwischen 0,5 und 2,5 Euro), dürfte sich die Automatenindustrie jedoch erst der GeldKarte zuwenden, wenn die Händlergebühren gesenkt werden.

Geldkarten in Europa – Konkurrent oder Kooperation?

Neben dem ZKA in Deutschland beschäftigen sich auch in Frankreich, Großbritannien, Belgien und den meisten anderen Ländern entsprechende Organisation mit der Herausgabe von Geldkarten.

- Europay hat eine elektronische Geldbörse namens CLIP entwickelt, die zukünftig mit den Spezifikationen der CEPS und ECBS kompatibel sein soll.
- Chipknip in den Niederlanden XXX???
- SERMEPA ist der spanische Geldkartenherausgeber und arbeitet zusammen mit Europay an einer einheitlichen Spezifikation für Geldbörsen.
- Das CEPS (Committee for European Payment Systems) und ECBS (European Committee for Banking Standards) kooperieren auf europäischer Ebene bei der Spezifikation von Geldkarten im Gültigkeitsbereich der herkömmlichen EC-Karten.
- In Frankreich soll 1999 ein Feldversuch durchgeführt werden, bei dem mehrere Kreditinstitute Geldkarten herausbringen, die auf dem ZKA-Chip basieren.
- Gleiches gilt für Luxemburg. Hier wird eine elektronische Geldbörse (mit dem Chip der GeldKarte) unter dem Namen miniCash durch die Luxemburger Banken und Sparkassen seit März 1999 eingeführt. Sie lautet von Anfang an auf Euro lauten und ist zum Telefonieren an allen Kartentelefonen geeignet.

XXX Quellen???

5.3.4.2 Andere kartenbasierte Zahlungsverfahren

Natürlich steht die Geldkarte trotz aller Marktdurchdringung im Wettbewerb. Dies sind insbesondere die T-Card und PayCard der Telekom sowie das britische Verfahren „Mondex“, das auch in Deutschland eingeführt werden soll und ein weitaus höheres Maß an Anonymität bietet als die Geldkarte.

T-Card mit PayCard-Service

Dieses Verfahren der Telekom wurde in Verbindung mit der Deutschen Bahn 1997 als Bargeldlösung angekündigt. Ein weiterer Vorteil wäre gewesen, das Billing-System der Telekom zur Abbuchung der Zahlungen zusammen mit der Telefonrechnung einzusetzen (dann hätte die Karte allerdings keinen Bargeldcharakter mehr). Es sollte zunächst auf den Einsatz in Fahrscheinautomaten sowie (natürlich) als Telefonkarte abzielen. Nachdem

diese Karte sich bis Mitte 1998 nicht am Markt durchsetzen konnte (nur etwa 150.000 Exemplare bis April 1998), wurde es sehr still um dieses System.

Mondex

Das System Mondex existiert bereits seit einigen Jahren in Großbritannien und wurde 1995 in Swindon, UK getestet. Das Besondere an Mondex ist sein dem Bargeld sehr ähnlicher Charakter: Kunden und Händler (eigentlich: beliebige Teilnehmer, da alle über die gleichen Kartentypen verfügen) können offline, d.h. durch Zusammenschalten ihrer Lesegeräte Geldeinheiten übertragen. Das „Wallet“ ist hierbei ein kleines Lesegerät, das neben der Karte des Besitzers auch die des Transaktionspartners aufnehmen kann. Über eine Tastatur kann anschließend der Betrag von einer Karte auf die andere übertragen werden. Mondex-Karten lassen sich nicht nur über Bank-Terminals, sondern auch über Telefone aufladen.

Eine technische Voraussetzung ist damit bei Mondex eine fälschungssichere Hardware der Lesegeräte. Seit 1997 ist das Kreditkartenunternehmen MasterCard mehrheitlich an Mondex beteiligt. Auch in Deutschland ist die Einführung von Mondex geplant.

VisaCash

Dieses von Visa herausgegebene System wird international erprobt. In Deutschland setzt allein die Bankgesellschaft Berlin dieses System ein. Seit 1998 kündigen Visa und der ZKA die Entwicklung einer eigenen Karte an.

5.3.5 Elektronisches Geld

Das wohl interessanteste Verfahren gleich vorab: Ecash von DigiCash. Entwickelt wurde es von David Chaum, einem echten Crypto-Guru mit ZZ-Top-Bart, jedoch ohne Schlapphut.

DigiCash bietet mit Ecash ein münzbasiertes Verfahren an mit uneingeschränkter Anonymität für den Käufer auf der Basis blind geleisteter Signaturen durch den Bankserver [Chau92]. Münzen der jeweiligen Währung werden anhand eines *elektronischen Portemonnaies* verwaltet. Die Stückelung der Münzen entspricht 2er-Potenzen von 0,01. Auf diese Weise sind für die Bezahlung eines beliebigen Betrags B maximal $\log_2 B + 1$ Münzen erforderlich, was den Kommunikationsaufwand und vor allem den Aufwand für die rechenintensive Generierung und Verifikation von Münzen reduzieren hilft.

In seiner ursprünglichen Form besticht Ecash vor allem auch in der symmetrischen Anordnung von Kunden- und Händler-Wallet: Beide können die gleiche Software benutzen, die sowohl das Auszahlen als auch das Einziehen von Münzen steuert. An der Universität Hamburg hatten wir 1996 beispielsweise ein Börsenspiel entwickelt, welches – gekoppelt an die aktuellen Schlußkurse der Frankfurter Börse – allen Ecash-Besitzern weltweit die Möglichkeit bot, ihr Spielgeld für Aktienkäufe einzusetzen. Damit nahmen wir Geld ein. Irgendwann später entschloß sich der Mitspieler dann zum entsprechenden Tageskurs die Aktien wieder zu verkaufen, d.h. wir zahlten den betreffenden Betrag an ihn aus und aktualisierten das Depot. Die damit verbundene Softwareentwicklung war recht übersichtlich - insbesondere auch wegen der einfachen Handhabung der Wallet-Software.

Heute wird Ecash vornehmlich von Banken in unterschiedlichen Währungen angeboten: Die Deutsche Bank betreibt einen Feldtest in DM, während bei EUNet Finland, bei der XXX-Bank in Australien und der XXX-Bank in der Schweiz jeweils Feldtests in der Landeswährung durchgeführt werden. Ecash unterstützt nur einen geschlossenen Währungsraum, d.h. weder zwischen zwei Ecash-Räumen, die an die gleiche reale Währung gekoppelt sind, noch zwischen unterschiedlichen Realwährungen sind Ecash-Münzen automatisch konvertierbar.

Das ursprüngliche Protokoll wurde zudem für den Betrieb bei einigen Banken so erweitert, daß z.B. versehentlich gelöschte Münzen wiederhergestellt werden können.

XXX: Klären, ob damit immer noch Anonymität gewährleistet werden kann!!!

Das Ecash-Protokoll

Ein lokaler Münzvorrat des Käufers wird durch das individuelle Prägen von Münzen eingerichtet (Abb. XXX). Dieser Prozeß besteht zunächst aus der Generierung von „Münzrohlingen“ durch den Käufer selbst. Diese enthalten u.a. eine eindeutige Seriennummer. Die durch den privaten Schlüssel des Käufers signierte Münze wird

beim Bankserver eingereicht, so daß dieser anhand des öffentlichen Schlüssels die Zugehörigkeit zum Käufer verifizieren kann.

Bevor nun aber diese Münze dem Bankserver übermittelt wird, transformiert der Käufer die Datenstruktur in eine Form, die es dem Bankserver nicht erlaubt, die Seriennummer zu lesen. Aufgrund des kryptographischen Verfahrens der *blinden Signatur* kann die Bank jedoch trotzdem den Münzbetrag und die Seriennummer signieren. Der Bankserver protokolliert den Betrag in seiner Datenbank, um zu einem späteren Zeitpunkt die Münze beim Einlösen zu identifizieren und ihre Echtheit zu verifizieren. Vom Ecash-Konto des Käufers wird dabei der entsprechende Geldbetrag abgebucht. Nachdem der Käufer die Münze vom Bankserver zurückerhalten hat, transformiert er sie wieder in die ursprüngliche Darstellung. Dabei bleiben jedoch Betrag und Zertifikat unverändert (Schritt 3).

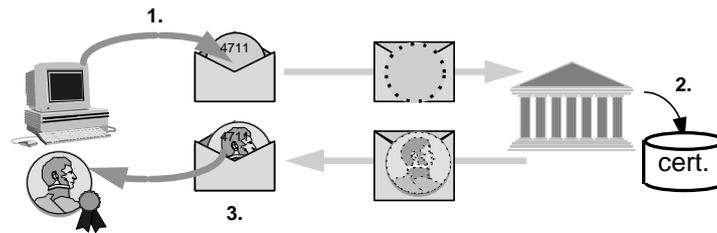


Abb. 15: Blind geleistete Unterschrift der Bank

Die Bank verfügt nun lediglich über die Information, *daß* der Käufer eine Münze abgehoben hat, jedoch nicht *welche*. Auch unter Kooperation der Bank mit dem Verkäufer kann nicht auf die Identität des Käufers geschlossen werden, da die Bank nicht über die jeweiligen Parameter für den Transformationsalgorithmus verfügt. Ein solches Protokoll zur Erzeugung blind geleisteter Unterschriften ist z.B. bei [PfWa95] beschrieben.

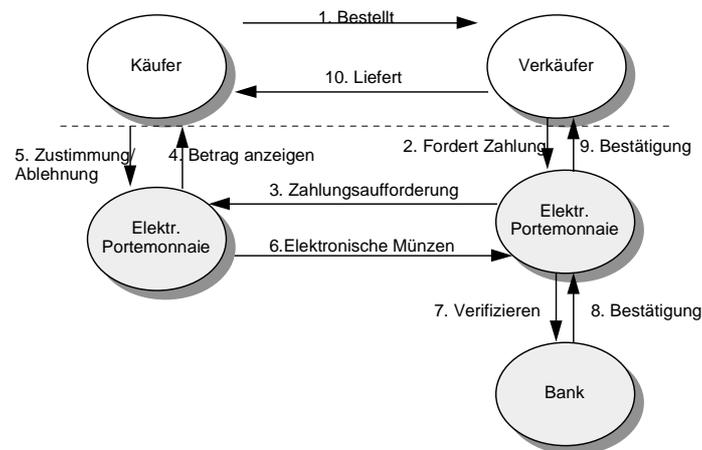


Abb. 16: Zahlungsprotokoll bei Ecash

Ecash-Transaktionen werden über elektronische Portemonnaies durchgeführt, die in einheitlicher Form beim Käufer und Verkäufer als individuell über Port-Nummern des Rechners adressierbare Prozesse vorliegen. Die Kommunikation zwischen Anwendungen (üblicherweise WWW-Browser und -Server) und elektronischen Portemonnaies erfolgt über eine Softwareschnittstelle seitens des Verkäufers (Vgl. Abb. 16). Wurde vom Verkäufer eine Bestellung entgegengenommen, wird sein elektronisches Portemonnaie veranlaßt, den betreffenden Münzbetrag vom Käufer einzuholen (Schritt 2). Diesem wird über die lokale Benutzerschnittstelle seines Rechners der Betrag und die Adresse des Verkäufers angezeigt (Schritt 4). Ist er einverstanden, bestätigt er die Zahlung und löst damit den Münztransfer aus. Anschließend kann der Verkäufer die Münzen beim Bankserver einlösen oder sie gegen neue wechseln (Schritt 7). Dabei verifiziert der Bankserver die Münzen und bestätigt im Normalfall deren Gültigkeit. Wenn der Verkäufer diese Bestätigung erhalten hat, kann er das Dokument oder die Ware an den Käufer ausliefern.

Hinter den Kulissen...

Was man als Kunde vom Ecash-Protokoll wahrnimmt, ist bereits beeindruckend. Noch interessanter ist jedoch der Algorithmus, der sich im Verborgenen abspielt - sozusagen hinter den Kulissen des Wallets. Der kryptogra-

phische Leckerbissen liegt in der Aufdeckung des Bösewichts im Fall des Double Spending. Es wird dabei nicht nur erkannt, *daß* dieser Fall eintritt, sondern auch, *wer* die Münze zweimal einsetzt: Schließlich könnte dies der Kunde, aber auch der Händler sein. Das Verfahren gestaltet sich folgendermaßen:

Neben der Münze, die vom Kunden an den Händler eingereicht wird, ist weitere Information verschlüsselt angehängt, die den Kunden identifiziert (z.B. seine Adresse, Personalausweis-Nr. o.ä.). Diese Information wird zunächst als Byte-String dargestellt und N-mal kopiert. Mit Hilfe eines sog. Secret-Splitting-Protokolls werden diese Strings jeweils in zwei Byte-Strings zerlegt (einen "linken" und einen "rechten" String). Aus diesen einzelnen Strings läßt sich nicht mehr auf die ursprüngliche Identitäts-Information zurückschließen - nur das Anwenden der Exklusiv-Oder-Funktion (XOR) auf beide Strings liefert die ursprüngliche Information.

Jedes der N String-Paare wird nun getrennt verschlüsselt, d.h. es gibt 2N Schlüssel, von denen jeweils einer auf den linken String und der andere auf den rechten angewendet wird. Zusammen mit der restlichen Münzinformation werden alle Strings an den Händler übertragen. Bevor dieser die Münze anschließend bei der Bank verifizieren läßt, fordert er zunächst je String-Paar einen Schlüssel vom Kunden an - entweder den linken oder den rechten. Dies erfolgt zweckmäßigerweise über einen Bit-String, bei dem 1 "linker Schlüssel" und 0 "rechter Schlüssel" bedeutet. Zum Anwenden der XOR-Funktion fehlt also jeweils eine Hälfte der Paare.

Die Münze wird zusammen mit den N halb-entzifferten Stringpaaren an die Bank weitergeleitet. Diese prüft, ob ihre Signatur gültig ist und ob unter der Seriennummer bereits eine andere Münze eingereicht wurde. Ist dies nicht der Fall, liefert sie eine positive Bestätigung an den Händler. Ist es jedoch der Fall, verfügt sie bereits über die Schlüssel der vorherigen Einreichung. Dabei können zwei Situationen unterschieden werden:

1. Alle Schlüssel beider Einreichungen sind gleich verteilt (d.h. die Bit-Strings waren gleich). Dieser Zufall tritt extrem selten ein, nämlich statistisch bei jeder 2^N -ten Einreichung. Viel wahrscheinlicher ist in dieser Situation hingegen, daß der Händler selbst die Münze zweifach eingereicht hat (er kann ja nicht über die "anderen", vom Kunden generierte Schlüssel verfügen).
2. Wenn allerdings die Schlüsselverteilung der beiden Einreichungen nicht identisch sind, gibt es mindestens ein String-Paar, von dem beide Teile entziffert werden können. Ein anschließendes XOR bringt die Identität des Kunden ans Licht. Umgekehrt kann der Händler hier nicht betrogen haben, da er bei einem einmaligen Einsatz der Münze durch den Kunden niemals über beide Schlüssel eines Paares verfügen konnte.

Von hier an setzen organisatorische Maßnahmen ein, die ggf. sofort oder erst nach Häufungen von Betrugsfällen den Täter dingfest machen.

Bewertung

Ecash benötigt in seiner aktuellen Implementierung einen zentralen Bankserver – damit sind einer beliebigen Skalierbarkeit Grenzen gesetzt. Andererseits können mehrere Ecash-Domänen etabliert werden, so daß zur Verifikation einer "fremden" Münze ein Clearing-Protokoll zwischen Banken denkbar wäre. Einen Nachteil stellt die Notwendigkeit der Verifikation dar, der jedoch für alle münzbasierten Verfahren gegeben ist, da hier immer die Gefahr der Duplikation besteht.

Das Ecash-System erlaubt uneingeschränkte Anonymität für den Käufer, d.h. auch bei der Kooperation anderer involvierter Parteien (Netzbetreiber, Bank, Verkäufer) kann dessen Identität nicht aufgedeckt werden. Auf die dadurch entstehenden Gefahren weist z.B. [CaST95] hin.

Das Ecash-Protokoll ist nicht transaktional, d.h. Münzen können beim Zahlungsvorgang abhanden kommen mit der Folge, daß die Geldmenge sich ändert.

Bei Ecash besitzt weder die Bank noch eine andere Instanz außer den Transaktionspartnern Informationen über die Transaktionsdaten. Auch bei Ecash ist dem Verkäufer zwar der Inhalt der Transaktion bekannt, er kann ihn jedoch nicht mit der Identität des Käufers in Verbindung bringen.

Ecash läßt sich ohne Aufwand in eine EM-Infrastruktur integrieren, da elektronische Portemonnaies sowohl für Käufer als auch Verkäufer in gleicher Form als externer Prozeß genutzt werden können.

Für die Bank besitzt Ecash den Vorteil, daß trotz des Bargeld-Charakters des Systems das Buchgeld de-facto immer seitens der Bank erhalten bleibt - und damit auch der Zinsertrag, den die Bank mit dem Guthaben des Kunden (und des Händlers) realisiert. Ein kleines Rechenexempel soll dies verdeutlichen:

Durchschnittliche Bargeldhaltung pro Person:	DM		500,--
Anzahl Personen in der Bundesrepublik:	80		Mio.
Geldmenge M1:	40	Mrd.	DM

Durchdringung mit Ecash einer einzelnen Bank:	2%	=	0,8	Mrd	DM
Auf diesen Betrag entfallen Zinseinnahmen von:	DM 40 Mio. p.a.	(bei 5% Zinsen)			

Nimmt man an, daß bei einem eingespielten Betrieb die Kosten des Bankservers (oder besser: des erforderlichen Rechenzentrums) bei 10 Mio p.a. liegen sowie weitere mittelbare oder unmittelbare Kosten bei 10-20 Mio, so verbleibt doch eine recht akzeptable Kapitalrendite. Damit wird auch klar, daß die Nutzung von Ecash nicht nur eine Demonstration des Fortschritts ist, sondern eine nüchterne Rentabilitätskalkulation. Während nämlich andere Zahlungsverfahren, die auf Kreditkarten- oder Lastschriftverfahren basieren, lediglich die Benutzung des klassischen Buchgeldsystems rationalisieren, erschließt Ecash der Bank ein vollständig neues Zinspotential - denn die Bargeldhaltung ihrer Kunden nützt ihr wenig.

Ecash-Münzen sind zwischen den Kunden austauschbar. Ein technisches Problem von Ecash kann entstehen, wenn zur Verifikation der Münzen sehr viele Seriennummern gespeichert werden müssen. Da im Prinzip beliebig viele Kunden teilnehmen können, stellt diese strikte Zentralisierung irgendwann einen Engpaß dar. Ferner läßt sich Ecash auch mit Chipkartensystemen kombinieren.

5.3.6 Ecash-Feldtests der Banken

Da mit Ecash ausgegebenes digitales Bargeld anders als etwa die CyberCoins von CyberCash nicht bloß eine Verrechnungseinheit, sondern Bargeldcharakter hat, bei dem sicherzustellen ist, daß die Bundesbank nicht die Kontrolle über die Geldmenge verliert, drängt diese darauf, ein solches Instrument auch in den Händen der Banken zu belassen.

Ecash wurde bislang als Softwarelösung nur an Banken lizenziert. In Deutschland und Österreich sind dies die Deutsche Bank und die Bank Austria. Erstere betreibt seit geraumer Zeit einen Pilotversuch <<http://www.deutsche-bank.de>>, der mit 1.500 ausgewählten Kunden startete. Der Feldtest läuft seit Ende Oktober 1997. Inoffiziellen Quellen zufolge wollte die Deutsche Bank bis zu ca. 45.000 "aktive" Home-Banking-Benutzer sowie etwa 10.000 Bank-24 Kunden einbinden. Es wurde erwartet, daß damit ein Volumen von 2.000-5.000 "aktiver" Ecash-Benutzer erreicht werden konnte. Tatsächlich waren aber bis Ende 1998 nicht mehr als 12 Händler zu erreichen und nach [BöRi98] auch nicht mehr als 1.000 Kunden.

Für den Transfer zwischen DM und Ecash wird ein Giro-Konto der DB benötigt, dazu können pro Kunde mehrere Ecash-Konten eingerichtet werden (quasi als "Unterkonten"). Auf das Ecash-Konto kann per Überweisung oder Einzahlung Geld transferiert werden. Vom jeweiligen Ecash-Konto hebt man per Electronic Wallet Münzen ab.

Auf der Händlerseite wird das herkömmliche Wallet über CGI o.ä. eingebunden. Der Merchant-Server läuft auf AIX, Solaris, Linux, NT.

Etwa gleichzeitig mit dem Konkurs von DigiCash hat auch die Japanische Nomura-Bank angekündigt, ihren Feldtest zum Ende 1998 einzustellen.

Aktuelle Probleme beim Feldtest:

- Henne-Ei-Problem bez. Kunden und Händlern. Ohne ein vielfältiges Warenangebot besteht für den Kunden kein Interesse mitzumachen. Gleiches gilt für den Händler, wenn die potentielle Kundschaft zu begrenzt ist.
- Homogenität zwischen Kunden- und Händlerinteressen ist nicht gegeben. Nicht jeder der Kunden ist beispielsweise an professionellen Textur-Bitmaps interessiert, die angeboten werden. Ein besserer Ansatz wäre sicherlich, das "Boot-Strapping" des Feldtest aus einer bereits existierenden Online-Gemeinde heraus, z.B. aus dem Telelearning- oder Musikbereich.
- Alle(!) Transaktionen müssen mehrere Jahre Bank-intern gespeichert werden, was für ein wirkliches Micropayment-System illusorisch und kontraproduktiv ist. Eine solche Auflage gilt für Billing-Systemen wie z.B. MilliCent höchstwahrscheinlich nicht.

Mit einem neuen Konzept hat die Deutsche Bank nun einen Wiederanlauf vorgenommen. Hier werden eigene kleinspreisige Produkte der Bank (hauseigene Broschüren, Finanzsoftware und Werbepartikel wie Spielkarten, Uhren, Sekt etc.) angeboten. Die URL des Shops lautet: <http://www.deutsche-bank.de/shop>

Diese Artikel können mit Ecash oder Kreditkarte (SSL) bezahlt werden. Dabei ist es jetzt auch möglich, Pilot-

kunde zu werden, ohne ein Konto bei der Deutschen Bank zu eröffnen.

Weitere Nutzungsformen von Ecash

Ist damit die Idee der Micropayment-Systeme totgeboren? Nein! Denn ihr Einsatzbereich erstreckt sich über weit mehr, als bloß über das Internet zu bezahlen. Es ist ein intellektueller Spaß für den geeigneten Krypto-Fan, bei einer geselligen Kaminrunde einmal zu überlegen, wie sich beispielsweise Ecash für weitere Bereiche des täglichen Lebens einsetzen ließe. Hier ein paar Kostproben:

- **Bibliotheken.** Hier könnte man sich denken, daß jeden Monat das Leih-Budget der Bibliotheksbenutzer auf einen einheitlichen Maximalwert aufgefrischt wird. Mit diesem Budget kann ein bestimmtes Bücherkontingent ausgeliehen werden. Jedem Buch kann dabei ein Preis zugewiesen werden, der sich ggf. sogar abhängig von der Vorbestellung verändern kann. Schreibt ein Student gerade seine Diplomarbeit, kann er von seinen Kommilitonen eCash leihen und es ggf. im nächsten Monat "zurückzahlen". Man könnte sich auch vorstellen, daß zusätzliche Leih-Kontingente gegen Bezahlung in realer Währung nachgekauft werden können. Diese Anwendungsform von Ecash setzt genau dort an, wofür elektronisches Bargeld entworfen wurde - der Realisierung eines abgeschlossenen Währungsraumes. Über diesen Mechanismus wird eine schlichte Marktökonomie aufgespannt, die hilft, Spitzenlast zu glätten und eine faire Lastverteilung über Perioden, Personalressourcen und Bücher sicherzustellen.
- **Rechenzeit/Lastverteilung.** Als Generalisierung des Bibliotheksbeispiels läßt sich das Verfahren natürlich auf alle denkbaren Situationen der Lastbalancierung innerhalb geschlossener Benutzergruppen anwenden. Interessant ist hier die Verteilung von Informationen auf verteilte Datenbanken in Abhängigkeit von der Nachfrage, vgl. z.B. das System Mariposa [SDKL+94]).
- **Theater-Tickets.** Elektronische Münzen sind im Kern nichts anderes als Tickets. Sie werden von einem Veranstalter herausgegeben (der Betreiberbank), über eine Theaterkasse erworben (der Bank "um die Ecke"); sie sind anonym und werden vom Veranstalter beim Eintritt so entwertet, daß weder Fälschen noch anderer Betrug möglich ist. Insbesondere dem Fälschen wird in der Realität vor allem durch Hologramme o.ä. Maßnahmen vorgebeugt. Spielt man dieses Modell in eCash-Terminologie durch, lassen sich erstaunlich wenige Abweichungen finden. Allein die Handhabbarkeit der elektronischen Münze ist bei mobilen Anwendungen z.B. durch Nutzung von SmartCards zu gewährleisten. Damit eignet sich dieses Verfahren eher für Stammkunden, bei denen sich die Verwendung einer SmartCard schneller bezahlt macht. Schließlich bietet eCash wegen der "double spending detection" zudem noch den Vorteil, zusätzliche Betrugsversuche zu entlarven. [XXX URL auf Ponton-Projekt???)
- **Elektronische Briefmarken.** Wie im Abschnitt XXX erläutert, setzen Postunternehmen heute zunehmend kryptographische Verfahren ein, um elektronische Briefmarken zur Verfügung zu stellen, die dann als Barcode ausgedruckt werden können. Worin besteht nun der Unterschied zwischen einer elektronischen Münze und der Briefmarke? Erstere muß lediglich ausgedruckt werden. Dies ist jedoch ein leichtes für den geeigneten Softwareentwickler.
- **Elektronische Wahlen.** Jeder Wähler läßt sich einen der Strings "CDU", "SPD", „FDP“, "Grüne" etc. zusammen mit einer eindeutigen Seriennummer vom Wahlleiter blind unterschreiben. Der Wahlleiter erhält Informationen über jeden Wähler auf eine Weise, daß er ihn identifizieren kann, wenn dieser versucht, eine zweite Stimme abzugeben. Anschließend reicht der Wähler den String über einen anonymen Kanal beim Wahlleiter ein. Dieser verifiziert die "Münze" in üblicher Weise. Ein Double Spending kann nach dem Verfahren erkannt werden, wie es unter „E-Cash“ beschrieben ist. Am Ende des Tages wird die Anzahl der Münzen mit gleichem "Wert" (d.h. dem Namen der Partei) gezählt.

Nachdem wir nun elektronisches Geld als Allheilmittel fast wieder rehabilitieren konnten, stellt sich allerdings die Frage, ob nicht vielleicht die Juristen noch ihre Chance wittern, dieses Meisterstück kryptographischer Ingenieurskunst zu Fall zu bringen. Sie könnten darauf abheben, daß die Rechtsnatur elektronischen Geldes ungeklärt ist. Mit anderen Worten: Ich stehe morgens am Flughafen, möchte mir mein Last-Minute-Ticket nach Mallorca abholen und stelle fest, daß der Rechtsbeistand der Reiseagentur den Vollzug des Kaufes bestreitet. Die Argumentation wäre etwa so: Als Bankkunde habe seine Mandantin lediglich einen Haufen Bits und Bytes erhalten. Natürlich nimmt sie am Feldtest der XYZ-Bank teil, aber leider war die Internet-Verbindung zur Bank gestört, so daß weder die Verifikation der Münze, noch die Feststellung einer Fälschung aufgedeckt werden konnte. Ohne jede Rahmenvereinbarung über die Handhabung solcher Fälle ist wahrscheinlich niemandem richtig klar, welche Rechtssituation hier vorliegt. Folglich verschafft dies wiederum anderen Kollegen des Rechtsanwalts neue Betätigungsfelder, nämlich die Ausarbeitung wasserdichter Rahmenbedingungen, die dem oben genannten Abstreiten von vornherein vorbeugen. Der Kollege bei der Bank würde sich etwa auf folgendes berufen:

Was eigentlich der Bankkunde erhält, wenn er elektronisches Geld von seiner Bank abrufen, ist eine "Aneinanderreihung von Daten, die ihren Wert in einer 'gespeicherten' Zahlungspflicht der emittierenden Banken haben" ([Escher97], S. 1180). Folglich sollte man von "Wertdaten" in Analogie zu Wertpapieren sprechen, deren Struktur der Inhaberschuldverschreibung nach § 793 BGB nicht unähnlich sei. "In Anlehnung an die herrschende Lehre zum Wertpapierbegriff könnten daher Wertdaten als elektronische Datensätze über ein Privatrecht verstanden werden, deren Innehabung Voraussetzung für die Rechtsausübung gegenüber dem Schuldner ist" ([Escher97], S. 1181).

5.3.7 Andere Verfahren

5.3.7.1 Online-Inkassosysteme

Ein Ansatz, der sich sowohl von Bargeld-orientierten als auch von Buchgeldsystemen abgrenzt, ist die flexible Gestaltung von Verfahren zur Abrechnung und Rechnungslegung, die einerseits den hohen Verwaltungsaufwand beim Umgang mit Geldzahlungen vermeiden, andererseits aber versuchen, die Eintrittsbarrieren in die geschlossene Benutzergruppe, die sich mit der Einrichtung von Teilnehmerkonten ergibt, zu reduzieren.

Die Vorteile von Inkasso-Systemen sind folgende: Es ist kein Aufladen von Geldbörsen, keine Kontostandskontrolle und kein Anschluß des Händlers an ein Zahlungssystem-Betreiber erforderlich. Dabei sind zwei zukünftige Entwicklungen denkbar: 1. Ein Online-Dienst bietet sein existierendes Inkassosystem für externe Internet-Händler an oder 2. Eine Bank betreibt das Inkasso-System als Dienstleistung unabhängig von Online-Diensten (möglicherweise auch *für* diese). Laut [BöRi98] wird dieser Markt jedoch nicht als lukrativ und zukunftssträftig eingeschätzt.

T-Online-Billing

Das in Deutschland historisch bedeutendste System ist sicherlich T-Online, über das heute mehrere Millionen Teilnehmer in sehr effizienter Form Micro-Payments durchführen können. Beim T-Online-Inkasso geht man von 2% des Umsatzes zur Deckung der reinen Verbuchungskosten aus. Allerdings kann nicht davon ausgegangen werden, daß ein Abrechnungssystem wie das von T-Online mit 2% Gebühren kostendeckend, geschweige denn rentabel arbeitet. In [BöRi98, S. 84] wird geschätzt, daß dazu eher eine Gebühr von 6% erforderlich wäre (was im Micropayment-Bereich immer noch akzeptabel wäre). Für das T-Online-Internet-Billing – eine Erweiterung der Accounting-Software für Dritte – wurde ein Pilottest 1997/1998 mehrfach angekündigt, jedoch immer wieder verschoben.

MilliCent

Inkassosysteme werden heute international in Form der Produkte MilliCent (Digital) und MiniPay (IBM) angeboten. Ersteres ist dabei token- und letzteres kontenbasiert. Beide erfordern jedoch einen zentralen Billing-Server mit Schnittstelle zum Bankennetz (bei MilliCent „Broker“ genannt). Im Prinzip ist MilliCent nichts anderes als ein Multikunden-Inkassosystem.

MilliCent schaltet einen Zwischenhändler (Broker) zwischen die Geld-Bezahlung von Kunde und Händler. Anstelle also einen Euro an den Händler direkt zu entrichten, muß der Kunde zunächst Wertmarken in Höhe eines handhabbaren Betrags vom Broker kaufen (z.B. für DM 20,-). Diese Marken können dann flexibel und vor allem ohne Clearing durch Banken eingesetzt werden. Wenn der Händler einen größeren Betrag an Marken gesammelt hat, löst er diesen beim Broker in Euro ein. MilliCent ist also ein Mechanismus der die ansonsten hohen Transaktionskosten der Zahlung durch ein abgestuftes System aus Geldtransfers und leichtgewichtigen Zahlungen in „Scrip“ – so der Name für die Händlermarken – reduzieren hilft.

Im Hinblick auf die technischen Kosten der Bezahlung hat MilliCent in einem Rechenmodell nachgewiesen, daß selbst bei Transaktionsvolumina in Höhe 1/10 Cents immer noch ein wirtschaftlicher Betrieb möglich ist. Ausgeschlossen werden hierbei jedoch Anlaufkosten sowie alle weiteren organisatorischen Kosten.

Als „Scrip“ wird ein MilliCent-Koupon bezeichnet, den man aufgrund kryptographischer Maßnahmen nicht doppelt ausgeben, fälschen oder stehlen kann (jedenfalls nicht „ökonomisch“ erfolgreich). Scrip wird von jedem Händler „on the fly“ mit niedrigem Overhead, ohne Netzwerkverbindung und ohne Datenbankzugriff validiert. Unterschieden wird Broker-Scrip und Händler Scrip, zwischen denen getauscht werden kann.

Die Wirtschaftlichkeit versucht, Digital mit folgender Rechnung nachzuweisen:

- Betriebskosten des Computers: 150.000 USD pro Jahr.
- Ein Jahr hat 30 Millionen Sekunden
- Zur Deckung der Betriebskosten sind somit ½ Cent pro Sekunde bei stetiger Last erforderlich, bei der üblichen Lastverteilung bis zu 25 Cent pro Sekunde.
- Unter der Annahme, daß 250 Transaktionen pro Sekunde durchgeführt werden können, sind dies 0,1 Cent pro Transaktion bei realer Last.
- Zu berücksichtigen sind allerdings technische Einschränkungen, da 250 TCP/IP-Verbindungen für einen einzelnen Server nicht realisierbar sind. Wir wollen daher davon ausgehen, daß durchschnittlich 0,5 Cents, als etwa ein Pfennig zur wirtschaftlichen Erbringung eines Broker-Dienstes erforderlich sind.

XXX

Durch die Verteilung der Fixkosten auf die einzelnen Transaktionen sollten sich Transaktionen mit dem Volumen von einem Cent realisieren lassen. Nicht berücksichtigt wurden jedoch die zusätzlichen Personalkosten sowie die mit der Einrichtung des Millicent-Servers verbundenen sonstigen Investitionskosten. Diese lassen sich nur decken, wenn ein immenses Volumen an Transaktionen bewältigt werden kann. Nehmen wir eine durchschnittliche „Gebühr“ von einem Pfennig pro Transaktion an, also 2,50 DM pro Sekunde bzw. 150,- DM pro Stunde und 3.600,- am Tag, dann deckt dies – grob geschätzt – die laufenden Kosten eines kleinen Büros mit 3-4 Mitarbeitern ab. Dabei sollte festgehalten werden, daß dieser Annahme 360.000 Zahlungstransaktionen (!) pro Tag, und ca. 10 Millionen im Monat zugrunde liegen. Dies entspricht in etwa den Spitzenreitern deutscher Online-Anbieter, hier allerdings gemessen in PageImpressions, d.h. jede im letzteren Fall wird jede Seite gezählt.

XXX

MilliCent wird daher insbesondere für den Online-Kauf kleinpreisiger Inhalte wie z.B. Audio-Clips, Nachrichten, Suchmaschinenzugriffe etc. angeboten.

Bisher wurde ein Feldtest seitens Digital durchgeführt, jedoch noch keiner in Verbindung mit Banken.

MilliCent braucht nicht den Druck der Notenbank zu fürchten, jedenfalls nicht in dem Maße, in dem dies bei E-Cash der Fall ist.

...

Weitere Informationen: <http://www.digital.com/PRW03M/>

Der MilliCent-Feldtest wurde laut Digital mit 10.000 Konsumenten und 45 Händlern durchgeführt. Dabei wurden über 100.000 Dollar and Scrip in Umlauf gebracht. Typische Artikel waren kleinpreisige Softgood wie etwa Music-Clips, Nachrichten, Screen Savers, Fotografien, 3D-Puzzles etc. Es heißt ferner, daß einer der Händler (Oxford University Press) selbst Artikel zu einem Preis von 0,2 Cent noch profitabel verkaufen konnte.

eCharge

Das Unternehmen eCharge nutzt den Telefon-Provider zur Abrechnung von Geldbeträgen. Über das Internet getätigte Käufe werden dabei einfach der Rechnung des Providers hinzugefügt und mit anderen Kosten gemeinsam monatlich abgerechnet. Dafür wird keine Kreditkarte o.ä. benötigt. Käufe sind auf Beträge bis zu 50 USD limitiert.

Wenn ein Kauf per eCharge durchgeführt wird, lädt der Kunde die Wallet-Software, beantwortet einige Fragen zur Person und bez. des Telefon-Providers und kann anschließend sofort Artikel kaufen.

eCharge läßt sich in das Microsoft Wallet als Zahlungsinstrument integrieren.

Weitere Informationen: <http://www.eCHARGE.com>

MiniPay

IBM's MiniPay wurde von Amir Herzberg am IBM Research Lab in Haifa entwickelt. Es sieht die einfache Integration eines Payment-Plug-In in den Web-Server vor, so daß ohne viel Aufwand das Bezahlen von Online-

Angeboten unterstützt wird. Das Geschäftsszenario sieht vor, das z.B. ein ISP als Verwalter des MiniPay-Kontos agiert und im Auftrag des Kunden Zahlungen durchführt. Ein Kunde verfügt dabei beim Bezahlen über ein Mini-Pay-Konto, für das er einen täglich aktualisierten Verfügungsrahmen erhält. Mit einer MiniPay-Bezahlung autorisiert er den Händler, den Zahlungsbetrag vom Kundenkonto abzubuchen. Dies erfolgt jedoch nicht sofort, sondern einmal täglich durch gegenseitiges Verrechnen der Zahlungsbeträge. ISPs schließen dafür weiterreichende Rahmenvereinbarungen.

Wie auch MilliCent zielt MiniPay darauf ab, die Transaktionskosten einzelner Zahlungen dadurch zu reduzieren, daß Abrechnungen zwischen Händler und Bank gesammelt und für alle Transaktionen eines Tages oder eines bestimmten Kontingents durchgeführt werden.

Weitere Verfahren

WebBill? (http://www.isoftware.de/1998/presse/pi_wb2.htm)

eCharge und die Telephongesellschaft Cable & Wireless bieten demnächst das Bezahlen von online geordneten Produkten via Telefonrechnung an.

5.3.8 Zusammenfassung

Im folgenden sind die untersuchten Systeme grob zusammengefaßt. Hier ist festzustellen, daß nur Ecash uneingeschränkte Anonymität des Käufers sicherstellt. Bei allen anderen Verfahren besteht entweder eingeschränkte Anonymität durch Pseudonyme oder keine, da einzelne Teilnehmer am Zahlungsverkehr (oder mehrere im Zusammenschluß) Transaktionen eines Teilnehmers vollständig nachvollziehen können.

Tabelle XXX: Klassifikation von Zahlungsverfahren

System	Beträge	Authentifizierung	Anonymität	Bargeld, Konto oder Buchgeld?
FirstVirtual	Makro	Outband	nein (Pseudonym)	Konto, Buchgeld
CyberCash	Makro	Online	nein	Buchgeld
SET	Makro	Online	nein	Buchgeld
Geldkarte	Micro	Online	nein	Buchgeld*
CyberCoin	Small	Online	nein	Buchgeld*
ecash	Small	Online	ja	Cash
MilliCent	Micro	Semi-Online	nein	Konto
Mini-Pay	Micro	Offline	nein	Konto
NetBill	Micro	Online	nein	Buchgeld
Mondex	Micro-Small	Offline	nein	Bargeld

*) Auch wenn diese Verfahren als „Bargeld-Verfahren“ charakterisiert werden, basieren sie de-facto jedoch auf Buchgeld, da immer auf Schattenkonten zurückgegriffen wird.

Wirtschaftlichkeit elektronischer Zahlungssysteme

Eines der undurchsichtigsten Gebiete ist beim elektronischen Zahlungsverkehr die Ermittlung der tatsächlichen Kosten, die mit der Durchführung einer Zahlungstransaktion verbunden sind. Weder läßt sich dies heute für laufende Feldtests korrekt ermitteln, noch für geplante Verfahren, deren Akzeptanz und Nutzungsweise zum heutigen Zeitpunkt noch gar nicht exakt prognostiziert werden kann. Es existieren weder Veröffentlichungen noch Hinweise der Feldtest-Betreiber, wie teuer es wirklich ist, CyberCash, eCash oder die Geldkarte zu betreiben. Insbesondere während der Einführungsphase dieser Systeme kann nicht davon ausgegangen werden, daß die

Betriebs- und Transaktionskosten der Systeme durch die jeweiligen Gebühren gedeckt werden. Allerdings muß für eine Bank und insbesondere für ein Unternehmen, das im wesentlichen von der Herausgabe elektronischen Geldes lebt, erkennbar sein, daß sich der Einsatz dieses Systems in der Zukunft rentieren wird.

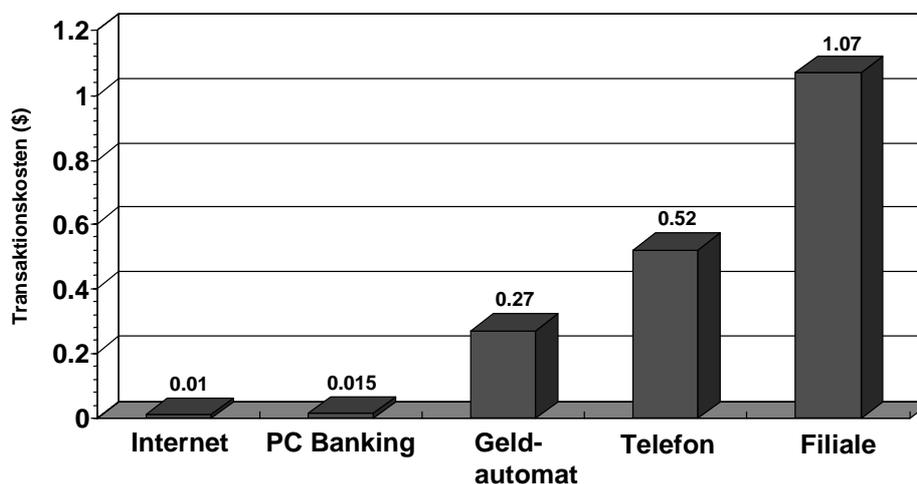
Zur Abschätzung der Kosten ist es nützlich, sich das Preismodell der Mark-Twain-Bank für die Nutzung ihres eCashes anzusehen (entnommen aus [BöRi98], S. 83). Händler- und Kundenseite werden hier separat betrachtet: In die Rechnung des Kunden fließen eine einmalige Registrierungsgebühr, monatliche Kontoführungsgebühren sowie transaktionsbezogene Gebühren von 11 Prozent ein (angenommen werden 5 Käufe im Wert von 10 USD). Auf der Händlerseite fallen – je nach gewählter Gebührenstruktur – bei 250 Verkäufen im Monat von ebenfalls 10 USD je Transaktion 0,28 bis 0,40 USD bzw. 2,8 bis 4 Prozent an [Himmelspach 1996, S. 13ff]. Diese Rechnung kann ebenso für die FirstVirtual Bank durchgeführt werden, dabei kommt man auf Transaktionsgebühren von 1,53 USD bzw. 15,3 Prozent für den Kunden und 0,50 USD bzw. 5 Prozent für den Händler.

Tabelle XXX: Gebührenvergleich eCash (Mark Twain Bank) und FirstVirtual

	eCash (Mark Twain Bank)		FirstVirtual	
	Kunde	Händler	Kunde	Händler
Annahmen	5 Einkäufe mit je 10 USD monatlich	250 Verkäufe mit je 10 USD monatlich	5 Einkäufe mit je 10 USD monatlich	250 Verkäufe mit je 10 USD monatlich
Gebühren pro Kauf	1,1 USD	0,28-0,40 USD	1,53 USD	0,50 USD
Anteil der Gebühren am Umsatz (Prozent)	11	2,8 - 4,0	15,3	4,95

Beide Banken mußten ihren Betrieb einstellen, da sich die Investoren der Banken aus dieser Geldanlage wegen mangelnder Rentabilität zurückziehen wollten. Diese wäre wahrscheinlich auf der Basis der genannten erst bei einer sehr viel höheren Beteiligung erreicht worden.

Eine Studie von Booz-Allen & Hamilton konzentrierte sich auf die Kosten verschiedener Banking-Schnittstellen des Kunden. Dabei ist der Betrieb einer Filiale mit direkter Kundenbetreuung mit 1,07 USD pro Transaktion (Geld abheben, Überweisungen etc.) am teuersten. Beim Telefon-Banking fällt mit 0,52 USD etwa die Hälfte und mit Bargeldautomaten nur ein Viertel (0,27 USD) an. Beim PC-Banking und Internet-Banking fallen die Transaktionskosten drastisch auf 1,5 Cent bzw. 1 Cent.



Quelle: Booz-Allen & Hamilton

Abb. 17: Kosten bei Zahlungstransaktionen über unterschiedliche „Schnittstellen“ einer Bank

In Deutschland kostet eine Kreditkartentransaktion den „Prozessor“ (als z.B. die GZS) ca. 0,50 DM. In den USA geht man von niedrigeren Kosten aus. Beim Electronic-Cash-Verfahren liegen die vom Händler zu zahlenden Gebühren durchschnittlich zwischen 0,10 DM und 1,00 DM bzw. 0,3 Prozent vom Umsatz und mindestens 0,15 DM. Schließlich liegen diese Händlergebühren bei Kreditkarten am höchsten: zwischen 0,8 und 8 Prozent. Bei Zahlungen ohne persönliche Identifikation (Telefon-Order) liegt die Spanne sogar zwischen 4 und 10 Prozent.

Damit variieren die konventionellen Verfahren stark in ihren Gebühren. Lediglich bei Kreditkarten kann jedoch davon ausgegangen werden, daß das Verfahren für die Betreiber rentabel ist. Im Bereich „electronic cash“ ist

dies eher eine Mischkalkulation und im Bereich der elektronischen Verfahren scheinen die Gebühren eher durch die Vorgaben der klassischen determiniert zu sein als durch die tatsächlichen Kosten.

Als Resümee der Untersuchung verschiedener Zahlungsverfahren kann festgehalten werden, daß sich voraussichtlich die traditionellen Systeme „Kreditkarte“ und „Lastschriftverfahren“ und die Geldkarte durchsetzen werden (abgesehen natürlich von der Banner-Werbung). Der eigentliche Grund liegt nicht in der besseren Effizienz dieser Systeme (dort liegt MilliCent beispielsweise im Vorteil), sondern in der vereinfachten Transition vom klassischen Verfahren in die Umgebung des Internet.

Eine Chance besteht möglicherweise langfristig für Systeme wie MilliCent und Ecash im Rahmen der Billig-Ökonomie. Sind die erforderlichen Vertrauens Technologien gegeben, ist durchaus denkbar, daß eine (Offshore-)Bank mit minimalen Betriebskosten in der Lage ist, auf der Basis von Ecash ein flexibles, wirklich anonymes und originäres Internet-Zahlungsmittel in Umlauf zu bringen.

6 Business-to-Consumer-Commerce

Neben dem elektronischen Bezahlen stehen beim B2C-Commerce die Themen

- Online-Kataloge
- Online-Shops sowie
- Profil-Management

im Vordergrund. Zu diesen Themen werden in diesem Kapitel die wichtigsten Eigenschaften und Entwicklungen dargestellt. Zuvor ist jedoch insbesondere beim B2C-Commerce zu berücksichtigen, daß die Durchdringung des privaten Bereichs durch das Internet in den nächsten Jahren zu unterschiedlichen Verschmelzungen von Zugangs- und Kommunikationstechnologien führen wird. Aus diesem Grund ist es zunächst sinnvoll, diese unterschiedlichen Technologien als Bestandteil eines Multimediums zu charakterisieren, daß am Ende dieser Entwicklung als grundlegende Electronic-Commerce-Infrastruktur dienen wird.

6.1 Die große Konvegenz

Bereits seit einigen Jahren wird die Konvergenz als nächster Wachstumsmotor für den Electronic Commerce gehandelt, nachdem das Internet sich als Infrastruktur zur Vernetzung von Workstations und Servern etabliert hat. Die Konvergenz bezieht sich auf das Verschmelzen der hute noch separaten Technologien Internet, Fernsehen und Telefonie. Diese drei Infrastrukturen basieren meist noch auf isolierten Netzwerken, Anwendungen und Inhalten. Sie lassen sich etwa folgendermaßen klassifizieren:

- **Fernsehen.** Fernsehen wird nach dem Broadcast-Prinzip betrieben mit wenigen Sendern als „Server“ und einer Vielzahl von Empfängern, die als „Thin Clients“ bezeichnet werden könnten, denn sie besitzen weder die Möglichkeit, lokale Zustände zu speichern, noch lokale Software auszuführen. Als Übertragungsmedium stehen Kabelnetze, Satelliten oder die terrestrische Ausstrahlung zur Verfügung. Auch beim klassischen Fernsehnetz ist wenig „Intelligenz“ für die Übertragung erforderlich. Traditionell spielen Fernsehnetze keine aktive Rolle bei der Ver- und Übermittlung von Inhalten. Investitionen können beim klassischen Fernsehen nur im großen Volumen erfolgen – dies gilt für die Kommunikationsinfrastruktur, für die Produktion von Inhalten (von der Werbesendung über Reportagen bis zur Filmproduktion) sowie für den Handel von Inhalten (Inhalte werden von Filmhändlern meist im Preisbereich zwischen einigen Millionen und mehreren hundert Millionen Euro angeboten). Der Netzbetrieb ist noch nicht liberalisiert, im wesentlichen tritt die Telekom als Betreiber auf. Einige Innovationen des klassischen Fernsehens bieten begrenzte Möglichkeiten der Interaktion, z.B. durch Videotext¹⁰. Jede weitere Form interaktiven Fernsehens erfordert die Integration eines anderen Netzes (Telefon oder Internet). Diese Integration reicht bis in die 80er-Jahre zurück und wurde eindrucksvoll bei der ersten internationalen Interactive-TV-Produktion „Piazza Virtuale“ anlässlich der Documenta 1992 demonstriert [Ponton XXX]. Beim Fernsehmedium herrscht heute noch die analoge Übertragungstechnik vor, es ist allerdings zu erwarten daß in den nächsten Jahren digitale Techniken wie DVB (Digital Video Broadcasting) dominieren werden. Spätestens im Jahre 2010 wird der Gesetzgeber diese Technologie europaweit vorschreiben. Damit sind für den TV-Bereich langfristig die Weichen zur Konvergenz mit den anderen Kommunikationsnetzen gestellt.
- **Telefon.** Das Telefonnetz erlaubt traditionell eine 1:1-Kommunikation seiner Teilnehmer. Telefonieren ist ein niedrigerpreisige Dienstleistung, zumal die Deregulierung dieses Marktes die Nutzungshürden auch weiterhin abbauen wird. In Deutschland ist das Vermittlungsnetz vollständig digitalisiert, lediglich die Anschlüsse sind zum größten Teil noch analog. Während beim Fernsehnetz keine Vermittlungstechnik erforderlich war, hat das Telefonnetz ständig wechselnde Verbindungsanforderungen zu erfüllen. Traditionell lag die wesentliche Komplexität hier seitens des Telekom-Providers. Auf der Client-Seite waren lediglich mit dem Telefon nur wieder „Thin Clients“ zu finden. Durch die frühe Digitalisierung des Telefonnetzes, bot es sich dem Telekom-Provider an, es rasch auch zur Übertragung digitaler Inhalte einzusetzen. Damit war die Integration von Fernvermittlungstechnologie als Grundlage zur Vermittlung von Internet-Inhalten kein großer Schritt mehr. Innovationen im Telefonsektor (Mobiltelefonie, ADSL, Drahtlose Kommunikation) erfolgt bereits seit einigen Jahren digital und mit der Möglichkeit, Integration-Protokolle zu integrieren.

¹⁰ Auch dies ist nur eine Internaktion zwischen Zuschauer und Fernseher, da sie nicht den Sender über das Fernsehnetz erreichen kann.

- **Internet.** Das Internet erforderte zur Kommunikation anspruchsvolle Software- und Hardware-System seitens aller Kommunikationspartner. Diese Systeme waren bis Anfang der 90er Jahre nicht nur kostspielig, sondern auch nur durch Spezialisten zu installieren und bedienen. Damit blieb es nur einem kleinen Kreis universitärer und industrieller Teilnehmer vorbehalten. In der „Vor-Web-Zeit“, also bis etwa 1994 herrschten ausschließlich e-Mail, FTP, Telnet sowie vereinzelt Gopher und X.500-Verzeichnisse als Kommunikationsdienste vor. Wider Erwarten der Pessimisten nahm trotz (eigentlich: *wegen*) der Kommerzialisierung des Internet die nutzbare Bandbreiten erheblich zu, so daß heute der Einsatz des Netzes zur Schaltung von Telefonverbindungen oder für das Video-Streaming zum Alltag gehört.

Bis zum heutigen Zeitpunkt ist der Anteil der „Cross-Over“ Inhalte – also nicht originär dem Medium entsprechende Inhalte – jedoch marginal. Neuere Anwendungen wie z.B. integrierte Call-Center (siehe unten) sind erst dann für breite Kundenkreise nutzbar, wenn die Telefon- und Datenkommunikation gleichzeitig über einen Anschluß erfolgen kann. Dies gilt heute nur für Firmenkunden oder Privatkunden mit ISDN-Anschluß. Geschäftsmodelle, die auf einer derartigen Integration beruhen, müssen folglich berücksichtigen, daß noch einige Jahre bei den meisten Verbrauchern ein analoger Telefonanschluß vorherrschen wird.

Dennoch ist durch die digitale Integration der drei Infrastrukturen ein ähnlicher Wachstumsschub zu erwarten, wie der durch die Standardisierung von Internet-Kommunikation durch e-Mail und HTTP vergleichbar ist. Am Ende dieser Entwicklung steht der breitbandige Kommunikationsanschluß in jedem Unternehmen und jedem Privathaushalt, der zum Preis heutiger Telefongebühren die Unterscheidung von Kommunikationsinfrastrukturen und Inhalten obsolet macht. Heutige, schmalbandige Kommunikation dürfte dann kostenlos oder zu niedrigen Pauschaltarifen möglich sein, da sie nur einen Bruchteil der zur Videokommunikation erforderlichen Kosten verursacht. Im folgenden werden einige aktuelle Entwicklungen beschrieben, welche jeweils die Konvergenz zwischen zwei der drei Infrastrukturen vorantreiben. Zunächst werfen wir dabei einen Blick auf die Zugangstechnologie zum Internet.

6.1.1 Zugangstechnologien zum Internet

Electronic Commerce findet im wesentlichen über das Internet oder zumindest über Internet-Protokolle statt. Damit ist noch nicht festgelegt, wie ein Teilnehmer in das System eingebunden ist. State-of-the-Art ist ein normaler Dial-In über Modem, ISDN-Verbindung oder Festverbindung. Auf der Anwendungsebene reicht beim B2C-Commerce auf der Kundenseite lediglich die Installation eines Browsers. Im Idealfall werden alle weiteren Komponenten als HTML-Seite oder Java-Applets geladen. An dieser Stelle sollen einige Alternativen erläutert werden, die in Zukunft einen möglicherweise viel bequemeren Internet-Zugang bieten. Diese sind:

- Set-Top-Boxen
- Kabelmodems
- ADSL
- Mobiltelefone

Alle neuen Zugangstechnologien sind durch die Konvergenz klassisch getrennter Medien gekennzeichnet: Entweder dient das Fernsehen als Trägermedium zur Internet-Kommunikation oder schnelle Internet-Anbindungen erlauben hochqualitative Multimedia-Übertragungen.

6.1.1.1 Set-Top-Boxen

Diese Systeme werden in Verbindung mit dem Fernsehgerät eingesetzt. Eine Set-Top-Box empfängt das Fernsehsignal und leitet es dann an den Fernseher weiter. Sie kann mit einer eigenen Fernbedienung gesteuert werden. Dabei hängt es von der Box ab, welche Funktionalität zur Bedienung zur Verfügung steht. Eine Set-Top-Box wie besitzt einen eigenen Prozessor und etwa die Rechenleistung eines 486er PCs. Da Festplatte, Monitor, Tastatur und kostspieliges Gehäuse fehlen, liegt der Preis bei einigen hundert Mark. Häufig sind Set-Top-Boxen über verschiedene Schnittstellen (SCSI, seriell) an die Außenwelt anbindbar. Zu unterscheiden sind Set-Top-Boxen für das analoge Fernsehsignal und solche für digitales Fernsehen.

NetBox von NetGem

Analog-Boxen, wie beispielsweise die von NetGem verwenden die Austastlücke bei der Übertragung des Fernsehsignals. Diese Lücke entsteht, wenn der Elektronenstrahl der Bildröhre zum Anfang der nächsten Zeile zu-

rückspringt. Da das Fernsehsignal kostenlos empfangen wird, kann ein Sender hier über 100 MB Daten pro Stunde übertragen. Pro Einzelbild sind dies immer noch etwa 1 KB, was für das Übertragen von Daten wie HTML-Seiten oder URLs ausreicht.

Die Box von NetGem besitzt einen i486er Prozessor mit 66-120 MHz Taktfrequenz sowie 4-8 MB Hauptspeicher. Als Betriebssystem dient ein modifizierter Linux-Kernel. Als Anwendungen stehen ein Web-Browser, E-Mail, Chat und in Zukunft weitere Internet-Clients zur Verfügung. Das besondere Merkmal der Box ist ein Modem für den Rückkanal. Die gesamte Box nimmt ungefähr den Raum einer Zigarrenkiste ein und ist damit sehr klein.

Erste Electronic-Commerce-Anwendungen wurden von der Telekom auf der Cebit '99 gezeigt. Hier hat die Firma Ponton Hamburg anhand eines Whitney-Houston-Clips demonstriert, wie passend zur Musik eine CD-Online bestellt werden kann [XXX Ponton-Settop-URL]. Dabei wird während der Fernsehsendung die URL des Online-Shops übertragen. Startet der Zuschauer den Web-Browser der Box, wird eine Produktseite zur CD eingeblendet. Über die Fernbedienung können Order- und Zahlungsinformationen eingegeben und der Bestellvorgang ausgelöst werden.

Wenn sich eine solche Technologie rasch durchsetzt, können die deutschen Nicht-PC-Haushalte (immerhin 75%) binnen kürzester Zeit und zu geringen Kosten an das Internet angebunden werden. In diesem Segment ist folglich für die Jahre 2000-2005 eine rasante Zuwachsrates zu erwarten. Neben Electronic-Commerce-Anwendungen sind beliebig viele weitere im Bereich des Interactive-TV zu erwarten. Insbesondere der Unterhaltungswert des Fernsehens kann dadurch gesteigert werden, was einen Fernsehsender wiederum kommerziell interessant macht.

D-Box

Die D-Box wurde ursprünglich von Nokia exclusive für das Digitale Fernsehen -- DF1 der Kirch-Gruppe entwickelt. Sie ist im Gegensatz zur Box von NetGem für den Empfang und die Darstellung digital übertragener Fernsehsendungen vorgesehen. Als Basistechnologie wird hier DVB -- *Digital Video Broadcasting* eingesetzt. DVB erlaubt die Übertragung digitaler Daten per Satellit, über das Kabelnetz oder auf terrestrischem Wege (Funk). Ein Satellitenkanal (ein sog. *Transponder*) erlaubt die Übertragung von 38 Mbit/s, die auf mehrere Fernsehkanäle aufgeteilt sind. Üblicherweise liegt die Bandbreite eines solchen Kanals bei 2-8 Mbit/s. Neben Fernsehsendungen kann diese Kapazität aber auch für den Broadcast von Daten eingesetzt werden. Die D-Box besitzt eine SCSI-Schnittstelle und ist damit auf die Integration mit dem PC vorbereitet. Somit besteht zumindest technologisch die Möglichkeit, größere Datenmengen effizient an eine größere Teilnehmerzahl zu verteilen (man denke z.B. an Windows 2000 ;-).

Das heutige Niveau der DVB-Anwendung liegt heute allerdings nur im Near-Video-on-Demand, d.h., zu vorbestimmten Sendezeiten werden verschlüsselte Filme übertragen, die von zahlenden Teilnehmern entschlüsselt werden können (Pay-Per-View). Dabei ruft man als Teilnehmer beim Call-Center von Premiere-TV an und gibt seinen Filmwunsch sowie seine Teilnehmerdaten (Kartenummer) durch. Die Bezahlung erfolgt zusammen mit den monatlichen Gebühren per Lastschrift. Vor der Ausstrahlung des Films wird ein Schlüssel an alle Empfänger verteilt, der ihnen das Dekodieren der Sendung erlaubt. Die D-Box enthält einen Chipkartenleser, in den die Kundenkarte eingeführt sein muß, wenn der Schlüssel übertragen und dort gespeichert wird.

Je nach Sendung wird also ein spezieller Sitzungsschlüssel verwendet. Die Übertragung des Schlüssels erfolgt über das gewöhnliche Kabel- oder Satellitennetz. Auf diese Weise wird sogar die Software der D-Box von Zeit zu Zeit aktualisiert. Hierbei ist nicht geklärt, ob Public-Key-Verfahren verwendet werden, um sicherzustellen daß der Sitzungsschlüssel an den richtigen Empfänger gelangt. Im anderen Fall könnte theoretisch jeder den Schlüssel abfangen, der die Hardware der Set-Top-Box entsprechend manipuliert.

In Prinzip ist die D-Box im Vergleich zur Box von NetGen funktional eingeschränkter, da kein Rückkanal besteht und auch keine Client-Software installiert ist. Eine Kombination der Merkmale beider Boxen könnte jedoch zu interessanten Electronic-Commerce-Anwendungen führen, da nun sowohl die Möglichkeit zum Bezahlen besteht wie auch zur Übertragung von Daten über den digitalen Broadcast-Kanal.

6.1.1.2 xDSL

Bisher wurde das Kupferkabel des Telefonanschlusses nur für Bandbreiten von bis zu 128 kbit/s (ISDN) genutzt. Diese setzen sich zusammen aus zwei B-Kanälen mit je 64 kbit/s und einem D-Kanal mit 16 kbit/s zur Übertragung von Steuersignalen. Prinzipiell liegt die maximale Bandbreite jedoch sehr viel höher und ist abhängig von der Länge und Qualität der Verbindung sowie von der Übertragungstechnik. XDSL steht dabei für Digital Subscriber Line -- also the digitale Telefonanbindung des Teilnehmers. Es werden folgende Verfahren unterschieden:

- HDSL (High data rate Digital Subscriber Line). Dieses Verfahren eignet sich für Distanzen bis zu 4.000 Meter. Die Übertragungskapazität liegt bei 768 kbit/s in beide Richtungen je Kabelpaar.
- SDSL (Single line Digital Subscriber Line). Hierbei wird die Telefonleitung nur in einer Richtung genutzt. Die Übertragungsrates liegt damit bei 1.544 kbit/s. SDSL eignet sich für Entfernungen von bis zu 3.500 Metern.
- ADSL (Asymmetric Digital Subscriber Line). „Asymmetrisch“ bedeutet hier, daß unterschiedliche Übertragungskapazitäten „downstream“ und „upstream“ (für den Rückkanal) vorliegen. Der Rückkanal erlaubt zwischen 16 und 640 kbit/s, während zum Teilnehmer hin 1,5 bis 9 Mbit/s übertragen werden können. Die Distanz kann dabei zwischen 3.000 und 6.000 Meter liegen. Allerdings lassen sich die hohen Raten nur bei kurzen Verbindungen erreichen.
- DSL-Lite erlaubt bis zu 8.000 Meter Distanz bei 384-1.500 kbit/s downstream und 128—384 kbit/s auf dem Rückkanal. Dabei kann die Distanz bis zu 8.000 m betragen.
- CDSL (Consumer Digital Subscriber Line) überbrückt 4.000—6.000 m bei 1 Mbps downstream und 128 Kbps auf dem Rückkanal.
- RADSL (Rate-Adaptive Digital Subscriber Line) paßt sich automatisch der Leitungsqualität an und erreicht bis zu 7 Mbp/s richtung Teilnehmer und 1 Mbp/s auf dem Rückweg.
- VDSL (Very high Digital Subscriber Line) bietet mit 13—52 Mbit/s bzw. 1,5—2,3 Mbit/s schließlich die maximale Rate. Dies ist jedoch nur bei extrem kurzen Verbindungen von bis zu 500—1.500 m möglich.

Zur Zeit führt die Deutsche Telekom mit T-DSL diese Technologie ein. Da bei den meisten Anwendungen und Kunden der Download überwiegt, basiert T-DSL auf dem asymmetrischen Verfahren von ADSL. Das Problem liegt dabei in der kontinuierlichen Aufrüstung der Vermittlungsstellen, die mehrere tausend Anschlüsse bedienen und nur Schritt für Schritt um die erforderliche Kapazität erweitert werden können. Aus vertriebspolitischen Gründen werden kurzfristig auch nur die eher langsamen Varianten angeboten, die preislich nicht zu sehr zum herkömmlichen ISDN in Konkurrenz stehen.

Die xDSL-Technik bietet eine ideale Grundlage zur mittelfristigen Konvergenz der bisher isolierten Fernseh-, Telefon- und Datennetze. In bezug auf den Electronic Commerce lassen sich die bisher diskutierten Infrastrukturen und Technologien auch auf Multimedia-Inhalte übertragen. Eine MP3-mit 5 MB läßt sich selbst bei DSL-Lite in wenigen Minuten laden bzw. in Echtzeit abspielen. Am oberen Ende des Spektrums von DSL-Lite lassen sich bei 1,5 Mbit/s nach MPEG-2 komprimierte Videos etwa mit heutiger Fernsehqualität übertragen. Dabei werden die Kosten bei weniger als 0,5 Euro pro Stunde liegen. Die Übertragungskosten der Audio-Datei (wenige Cent) fallen folglich nicht ins Gewicht.

6.1.1.3 Weitere Technologien

Kabelmodems

Kabelmodems bieten eine sichere, asymmetrische Verbindung über das Kabelfernsehnetz. Ein typisches Kabelmodem erlaubt Übertragungsraten von 30 Mbit/s und 2,56 Mbit/s auf dem Rückkanal. Die Übertragungskapazität der Modems trägt jedoch, da das Netz traditionell nur für die Übertragung zum Empfänger ausgelegt ist und daher zunächst ist ein erheblicher Aufwand zur Umrüstung der Verteilknoten erforderlich ist. Ebenfalls ist die baumartige Verteilerstruktur der Fernsehkabel problematisch: hier können sich alle angeschlossenen Empfänger lediglich nur das eine Übertragungskabel teilen, an dem sie partizipieren. Wenn dies einige hundert Haushalte sind, fällt die jeweils verbleibende Bandbreite auf weniger als die des DSL-Lite.

Stromnetz

Aus das Verteilnetz der Stromversorger läßt sich zur Datenübertragung nutzen. XXX

6.1.2 Next Generation Internet und Multimedia-Protokolle

Das Next Generation Internet (NGI – <http://www.ngi.gov>) und das Internet-2 (I2 – <http://www.internet2.edu/>) sind zwei eng verbundene US-Projekte, die versuchen, Bandbreiten- und Kommunikationsprobleme des heutigen

Internet zu lösen. Diese Entwicklung wird gemeinsam von Universitäten, der Regierung und der Industrie vorangetrieben. Vor allem steht eine Erweiterung der Dienstgüte bei hundert- bis tausendfach schnelleren Ende-zu-Ende-Verbindungen im Vordergrund. Insbesondere sind dies Multimedia-Integration, Interaktive Multimedia-Dienste und Multimediale Telekooperation. Diese Technologien gelten als Grundlage des Distance Learning sowie den lebenslangen Lernen – insbesondere im internationalen Kontext.

Das NGI besteht aus zwei neuen Netzen: eins für die Forschungsgemeinde mit über 100 angeschlossenen Knoten und 100 Mbit Übertragungsrate und einem zweiten, das nur zehn Knoten vorbehalten bleibt mit 1 Gbit Übertragungsrate.

Das Internet-2 schließt folgende Technologien ein:

Switch/Router-Technologien zur Unterstützung des neuen IP-6-Protokolls bei 622 Mbit/s und mehr

Möglichkeiten zur Übertragung von Echtzeitdatenströmen durch fester Reservierung von Bandbreiten. Steigerung der Zuverlässigkeit bei der Übertragung von IP-Paketen

I2 wurde entworfen, um multimediale Daten sicher und ohne Engpässe bei der Übertragung auszutauschen. Dies ist insbesondere bei Distance-Learning-Anwendungen erforderlich, wenn eine größere Zahl Empfänger bei Multicast-Anwendungen erreicht werden soll.

Auf der Middleware-Ebene wird eine Architektur entwickelt, die auf der Basis objektorientierter und komponentenbasierter Softwaretechnologien Funktionen vorsieht, die über spezielle APIs den Umgang mit Verbunddokumenten, Metadaten und Multimedia-Verbindungsparametern erlauben.

Multimedia-Kommunikationsstandards

Der DVB-Technologie liegt als Übertragungsstandard MPEG-2 zugrunde (Moving Pictures Expert Group). MPEG-2 erlaubt die Übertragung komprimierte Video- und Audiodatenströme. Es wird eingesetzt zur Codierung von DVD-Inhalten sowie für das digitale Fernsehen. Bereits heute existiert die Möglichkeit, neben Multimedia-Daten auch IP-Daten per DVB-broadcast zu übertragen. Technologien wie Open TV (www.opentv.com) erlauben dabei auf der Seite des Senders einen IP-basierten Kommunikationskanal (Socket) zu öffnen und Daten wie z.B. HTML-Seiten zu übertragen. Jeder Empfänger, der neben dem DVB-Decoder auch über eine Open-TV-Software verfügt, kann diese Information verarbeiten. Open-TV-erlaubt somit beispielsweise, zu Fernsehsendungen eine passende Kollektion von HTML-Seiten zu übertragen. Diese können auf der Workstation oder Set-Top-Box des Empfängers gespeichert und mit Hilfe eines Web-Browsers angesehen werden. Ähnlich der Übertragung beim Videotext werden die HTML-Seiten zyklisch ausgelesen, so daß der Empfänger innerhalb einer bestimmten Wartezeit wieder die erste Seite lädt (Karussell-Verfahren).

Als Nachfolger des bereits seit einigen Jahren existierenden MPEG-2-Standards wurde im Dezember 1998 MPEG-4 von der ISO verabschiedet (Details sind unter <http://www.csel.it/> und <http://www.iso.ch> zu finden). MPEG wurde entwickelt, um eine nahtlose Integration von Video-, Audio- und Web-Daten bei Rundfunk- und Interaktiven Anwendungen zu erreichen. Es kann sowohl beim digitalen Fernsehen als auch im WWW eingesetzt werden.

MPEG-4 erweitert seine Vorgänger MPEG-1 und MPEG-2 um folgende Eigenschaften:

- Integration natürlicher und synthetischer Elemente als „Objekte“, die aufgenommene Szenen oder Audio-Daten beinhalten oder synthetisiertes Material wie ein Musik ein animiertes Gesicht oder eine animierte 3D-Szenen).
- Übertragung von 2D- und 3D-Inhalten.
- Unterstützung unterschiedlicher Formen der Interaktion.
- Kodierungstechnik für schmalbandige und breitbandige Übertragungskanäle (zwischen 2 kbit/s und 64 kbit/s für Audio und zwischen 5 kbit/s und 5 Mbit/s für Video).
- Schutz und Verwaltung von Eigentums- und Verwertungsrechten am Inhalt

MPEG-4 erweitert gleichzeitig Eigenschaften des VRML-Standards (Virtual Reality Markup Language) durch die Einbindung von Echtzeit-Übertragungen in 3D-Szenen. Video- und Audio-Datenquellen werden dabei per URL identifiziert. Multimediale Szenenbeschreibungen sind ebenfalls als Teil des MPEG-4-Datenstroms integriert.

Beispielsweise können über MPEG-4 Lerninhalte übertragen werden, die sich aus folgenden Komponenten zusammensetzen:

- Eine Kamera nimmt einen Dozenten in einem Virtuellen Studio auf. Dabei wird sein Körperumriß aus dem Hinergrund herausgefiltert und in eine synthetische Szene eingeblendet. Der Dozent kommentiert die Lerninhalte in natürlicher Sprache.
- Die synthetische Szene beruht auf einem 3D-VRML-Modell, welches auf der Empfängerseite über Steuerdaten der MPEG-4-Übertragung mit der Kameraeinstellung für den Sprecher synchronisiert wird.
- Auf eine Leinwand in der 3D-Szene wird beim Empfänger ein synthetischer Video eingeblendet, der mit synthetischer Musik unterlegt ist. Gleiches gilt für den Sprachkanal zur Präsentation. Hierbei können unterschiedliche Sprachen interaktiv vom Empfänger ausgewählt werden. Alternativ lassen sich auch Untertitel einblenden.
- Schließlich ist neben der Leinwand ein 3D-Anschauungsmodell in die Szene projiziert, das vom Betrachter interaktiv manipuliert werden kann.
- Durch Bedienelemente wie Maus, Tastatur und Spracheingabe kann der Betrachter über einen Rückkanal auf den Inhalt Einfluß nehmen. Dabei wird entweder eine Internet-Verbindung oder das Fernseh-Kabelnetz direkt genutzt.

Im Hinblick auf Electronic-Commerce-Anwendungen erschließen sich hierbei unterschiedliche Möglichkeiten der Produktion, Integration, Kombination, Personalisierung, Lokalisierung, Verbreitung und Abrechnung kommerzieller Inhalte. Dies kann sowohl beim Distance-Learning, beim Business-TV oder beim kollaborativen Arbeiten wie auch zu Unterhaltungszwecken oder für massiv-interaktive Online-Spiele eingesetzt werden.

6.1.3 Mobilfunknetze

Marktteilnehmer sind zunehmend mobil in dem Sinne, daß sie sich an wechselnden Orten befinden oder vor allem auch während der Reise Kontakt zum Netz halten möchten. Im folgenden wird „Mobilkommunikation“ von der „drahtlosen Kommunikation“ (Ad-hoc-Netze oder Funknetze zur Überbrückung der „letzten Meile“) unterschieden, die nicht notwendigerweise reisende Teilnehmer unterstützt.

Das besondere Problem liegt bei der Mobilkommunikation in

- der heute noch reduzierten Bandbreite von Mobilverbindungen
- in der Möglichkeit für Dritte, die Übertragung abzuhören
- sowie in der niedrigen Übertragungsqualität.

Der heutige, europäische GSM-Standard für Mobiltelefone erlaubt lediglich eine Übertragungsrate von 9,6 kbit/s. Nach dem Analogstandards der ersten Generation, die seit 1979 genutzt werden, liegt mit GSM seit 1990 ein digitaler Standard vor, der im Frequenzbereich von 900 bzw. 1800 MHz eingesetzt wird. Systeme der dritten Generation werden ab ca. 2002 zur Verfügung stehen und Übertragungsraten von 144 kbit/s auf der Reise und bis zu 2 Mbit/s stationär zulassen. Darüber hinaus sind sie so entworfen, daß Benutzern integrierte, multimediale Dienste angeboten werden können (Sprache, Daten, Grafik, Video). Der Europäische Standard der dritten Generation ist bekannt als UMTS (Universal Mobile Telecommunication System). Zukünftig ist zu erwarten, daß dieser Standard als ein Teil in ein weltweites System einfließen wird, das es Benutzern erlaubt, an jedem Ort der Welt mit der verfügbaren Bandbreite zu kommunizieren. Das Mobilgerät wird sich dann aus dem verfügbaren Angebot das schnellste bzw. preiswerteste Kommunikationsmedium auswählen. Diese könnten z.B. GSM, UMTS, Satellitenkommunikation oder auch lokale drahtlose lokale Netze nach dem DECT- oder IRDA-Standard sein.¹¹UMTS wird sowohl Echtzeitkommunikation unterstützen (z.B. für Sprach- und Videoübertragungen) als auch asynchrone Kommunikation (e-Mail, WWW).

UMTS wird in unterschiedlichen Varianten zur Verfügung stehen: in kleinen, sog. „Picozellen“ (im Büro oder in der Wohnung) kann die maximale Bandbreite von bis zu 2 Mbit/s ausgenutzt werden. Picozellen werden zu Mikrozellen zusammengefaßt, die einige Quadratkilometer abdecken. Auf diese Zelle greift das Mobilgerät zurück, wenn der Hausbereich verlassen wird. Hier steht eine Übertragungsrate von bis zu 384 kbit/s zur Verfügung. Pico- und Mikrozellen werden wiederum von Makrozellen Mit 144 kbit/s abgedeckt die etwa der Zellengröße des heutigen GSM-Netzes entsprechen. Schließlich werden abgelegene Gebiete, die von keinem terrestrischen System abgedeckt werden können, über satellitengestützte Systeme wie das heute bereits verfügbare Iridium einge-

¹¹ DECT – Digital Enhanced Cordless Telecommunications, IRDA – Infra Red XXX

bunden.

Einige der zukünftigen Kommunikationsprotokolle im Mobilfunkbereich sind in der folgenden Tabelle aufgeführt:

Tabelle XXX: Aktuelle Standards der Mobilkommunikation

Technologie	Zellengröße	Verzögerung < 10 ms	Abdeckung
TDMA IS-136A (Time-Division Multiple Access)	Makro	Nein	National, Stadtteil, Stadt
CDMA IS-95A Code Division Multiple Access	Makro	Nein	National, Stadtteil, Stadt
GSM (Global System for Mobile Communications)	Makro	Nein	National, Stadtteil, Stadt
PACS (Personal Access Communications System)	Makro	Ja	Stadtteil, Stadt
W-CDMA (Wide-band Code Division Multiple Access)	Macro	Nein	National, Stadtteil, Stadt
AMPS/NAMPS (Advanced Mobile Phone System)	Makro	Ja	National, Stadtteil, Stadt
DECT Digital Enhanced Cordless Telecommunications	Pico	Nein	Stadt
PHS (Personal Handphone System)	Pico	Nein	Stadt
Satellite	Global	Hoch	Global

Das UMTS-Forum (<http://www.umts-forum.org>) hat als internationales Standardisierungsgremium sagt für das Jahr 2000 einen Weltmarkt von 426 Millionen Benutzern von Mobilkommunikation vorhergesagt. Über 2005 wird diese Anzahl bis zum Jahre 2010 auf 940 Millionen und 1,7 Milliarden steigen. Auf Westeuropa entfallen dabei für das Jahr 2005 200 Millionen Benutzer, von denen etwa 32 Millionen mobile Multimedia-Nutzer sein werden. Das Marktvolumen für mobile Multimediadienste wird mit 24 Milliarden Euro und 3.800 Millionen Megabyte pro Monat prognostiziert.

6.1.4 Call-Center

Call Center finden ihren Einsatz bei beratungsintensiven Produkten und Transaktionsphasen. So kann die Aufgabe eines Call-Centers – entlang der Phasen – in der Produktinformation, der Kauf- oder Konfigurationsberatung, dem Abschluß eines Vertrages oder in After-Sales-Bereich liegen. Im letzten Fall kommt die Aktualisierung von Vertragsdaten, die Benutzerhilfe oder der anschließende Buchungs- bzw. Bestellvorgang in Frage. Call-Center werden heute in unterschiedlichen B2C- und B2B-Szenarien eingesetzt. Im folgenden ist eine Auswahl von Branchen und Aufgaben beschrieben:

- *Pre-Sales-Support*: Online-Autohändler beraten den Kunden bez. der verfügbaren Varianten und Zusatzkomponenten auch Fragen der Finanzierung und der Kaufabwicklung können online vereinbart werden.
- *Kontoführung bei Online-Banken*. Aufgrund rechtlicher Bestimmungen ist die Eröffnung eines Kontos noch nicht vollständig online möglich, jedoch bieten Online-Banken heute das gesamte Dienstleistungsportfolio zur regulären Kontoführung an.
- *Online-Verkauf von Versicherungspolicen*. Bei einfachen Verträgen wie z.B. bei Hausrat-, KfZ-oder Auslandskrankenversicherungen besteht die Möglichkeit, den Verkauf online über ein Telefongespräch abzuwickeln.
- *Support*. Softwarehersteller bieten in der Regel ihre Support-Dienstleistung über ein Call-Center an.

Alle diese Leistungen waren natürlich auch schon vor der Welle der Call-Center-Einführung seit Mitte der 90er Jahre möglich, die wesentliche Innovationen, die diesen Begriff prägte, lagen dabei in folgenden Rationalisierungseffekten:

- *geographischen Unabhängigkeit*: Viele deutsche Unternehmen verlagern ihr Call-Center ins Ausland. So ist Oracle-Direkt beispielsweise in Irland ansässig. Auch in Namibia, wo eine deutschsprachige Minderheit lebt,

ist der Betrieb ein lukratives Geschäft. Prinzipiell ist der Einfluß der Telekommunikationskosten inzwischen so gering geworden, daß diese Dienstleistung fast von jedem Ort der Welt aus angeboten werden kann.

- *Software-Integration*: Call-Center sind nicht nur über das Telefonnetz mit dem Unternehmen integriert sondern vor allem über ihre Datenbanken. Auch die Integration mit dem Internet ist heute Stand der Technik, so daß Kunde und Agent gemeinsam im Internet browsen können (siehe weiter unten).
- Es kann ein *Kundenprofil* angelegt werden, welches neben den üblichen Daten zur Identifikation auch die Historie früherer Kontakte einschließt. Wenn ein Kunde anruft, wird er zunächst identifiziert und anschließend zusammen mit „seinen“ Daten an einen geeigneten Agenten weitervermittelt. Dieser verfügt dann über die nötige Hintergrundinformation.
- *Agentenprofile* helfen, den Kunden durch einen versierten Mitarbeiter mit dem passenden Kenntnisprofil zu unterstützen. Hierzu ist wiederum eine enge Integration zwischen dem Telefonnetz und der Call-Center-Software erforderlich.
- *Basisprodukte und -dienstleistungen*. Schließlich braucht die Call-Center-Infrastruktur nicht vollständig neu entwickelt werden, da Unternehmen wie z.B. Micrologica, Accent oder Siemens wesentliche Komponenten als Produkte anbieten. Dennoch ist die erforderliche Investition für das Customising dieser Technik nicht zu unterschätzen. Sie kann jedoch vermindert werden, wenn die gesamte Call-Center-Dienstleistung an ein Unternehmen ausgelagert wird, das sich als Service-Betreiber für mehrere Auftraggeber gleichzeitig einsetzen läßt.

Die Konvergenz von Telefonie, Internet und Softwaresystemen zeigt sich vor allem in der Architektur eines Call-Centers (Abb. XXX). Hierbei ist bei modernen Systemen folgendes Szenario denkbar: Ein Kunde surft mit seinem Browser im Online-Shop eines Anbieters. Dort findet er beispielsweise das Angebot eines Autohändlers, über das er sich weitere technische Informationen einholen möchte (Schritt 1 in Abb. XXX). Er drückt auf der Seite mit der Produktspezifikation einen „Call-Me“-Button, der auf den Web-Server des Call-Center verweist. Im nächsten Schritt wird der Web-Server des Call-Centers kontaktiert, der die Informationen an den Server des Call-Center weiterleitet. Dieser Server wird über die Parameter der URL informiert, an welchem Produkt der Kunde interessiert ist. Auch eine Kunden-ID kann übergeben werden, wenn er sich registriert hat.

Die Web-Call-Center-Software steuert mit dieser Information den PABXXXX?? des Call-Centers an, um eine Telefonverbindung zwischen dem Kunden und einem Agenten zu schalten (Schritt 2). Bereits hier besteht die Möglichkeit, den Kunden mit einem „passenden“ Agenten in Verbindung zu bringen, damit seine Anfrage schnell beantwortet werden kann. Hierbei gilt es, das Profil der Produktinfo-Seite mit dem der verfügbaren Agenten abzustimmen. Nachdem eine Telefonverbindung hergestellt wurde, besteht zunächst die Möglichkeit, ein Beratungsgespräch zu führen (Schritt 3). Der Agent im Call-Center erhält dazu die Web-Seite des Kunden in seinem eigenen Browser. Bei speziellen Fragen, die sich auf die Web-Seite des Anbieters beziehen, ist es nun erforderlich, daß das Gespräch unter der Integration des Internet weitergeführt wird: Da der Kunde sich für ein spezielles Detail in der technischen Spezifikation interessiert, möchte er mit dem Agenten zusammen auf die Web-Seite des Anbieters „surfen“. Dazu ist jedoch eine Synchronisation erforderlich, die beiden Parteien die gleiche Web-Seite zur Verfügung stellt. Dies geschieht, indem Kunde und Agent über den Web-Server des Call-Centers indirekt auf den des Anbieters zugreifen. Zu diesem Zweck wird ein *Web-Agent* eingesetzt, der zwei Browser gleichzeitig mit dem gleichen Inhalt versorgt (Schritt 4). Dabei navigiert einer der beiden durch die Seiten des Anbieters, so daß seitens des Web-Agents nur ein HTTP-Request abgesetzt wird. Erst wenn diese Seite an den Web-Agent ausgeliefert wurde, leitet er sie an beide Browser weiter. Dabei können entweder Push-Technologien erforderlich sein (für den passiven „Mitsurfer“) oder er klickt auf die gleichen Links der Seite wie der aktive Surfer, wobei jedoch die verwendeten URLs durch Verweise auf den Web-Server des Call-Centers ersetzt wurden, so daß dort ein Serverprozeß angestoßen werden kann, der auf die HTML-Seite des aktiven Surfers wartet.

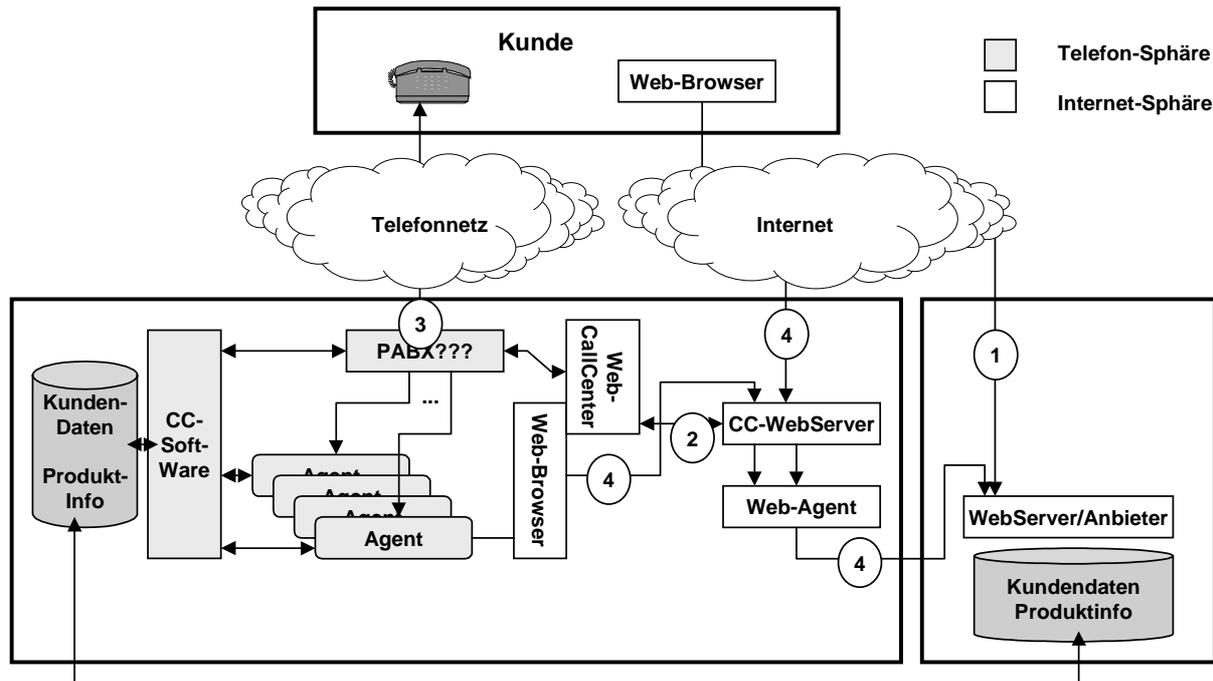


Abb. 18: Komponenten eines Call-Centers

Die beschriebene Integration eignet sich insbesondere für den B2B-Bereich, da hier beim Kunden die Internet-Verbindung unabhängig ist von der Telefonleitung. Bei Privatkunden ist das Problem zu lösen, daß beide Kommunikationsverbindungen exklusiv die Telefonleitung blockieren (nur ein geringer Teil der Privatkunden verfügt über eine ISDN-Nebenstelle). Einen Ausweg bietet hier die Internet-Telefonie, bei der der Sprachkanal gleichzeitig zur HTTP-Kommunikation aufgebaut werden kann. Diese Lösung erfordert jedoch beim Kunden die nötige Ausstattung zur Sprachkommunikation.

Call-Center sind somit ein typisches Beispiel für den heutigen Stand der Konvergenz: Während die Kommunikationskanäle noch getrennt gehalten werden, erfolgt bereits ein hohes Maß an Integration seitens der Endpunkte. Bereits diese Integrationsstufe hat zu einem rasanten Wachstum des Dienstleistungsmarktes im Bereich Call-Center geführt.

6.1.5 Zukünftige Zugangstechnologien und Electronic Commerce

Wählen wir das Jahr 2010 als Basis für ein Szenario: weite Teile der Bevölkerung verfügt über die Möglichkeit, nahezu permanent an das Internet angebunden zu sein. „Internet“ ist hier weniger als Kommunikationstechnologie sondern als „Weltöffentlichkeit“ aufzufassen. Die Kosten der multimedialen Kommunikation sind im Festnetzbereich auf einen Bruchteil der heutigen Kommunikationskosten gefallen. Gleiches gilt für die breitbandige Mobilkommunikation. Schmalbandige Mobilkommunikation ist nahezu kostenlos. Der Teilnehmer nimmt nicht mehr wahr, ob er gerade über eine drahtlose LAN-Verbindung oder eine Mikrozone angebunden ist. Der Laptop wählt automatisch die preiswerteste Verbindung für den erforderlichen Verbindungsmodus aus. Es ist damit belanglos, ob sich der Teilnehmer gerade im Café auf Mallorca, in der Wohnung in Hamburg oder im Taxi auf einer Geschäftsreise in den USA befindet – lediglich die Bandbreite kann zwischen 128 kbit/s und einigen Mbit/s variieren.

Mobilität

Zunächst einmal wird das Mobilgerät mit der heutigen Funktion der SmartCard verschmelzen. Genauso wie letztere als physisches Instrument den Besitzer gegenüber dem Provider bzw. dem Kommunikationspartner authentifiziert, kann diese Funktion von einem PDA oder Notebook übernommen werden, in dem die Krypto-Funktion fest installiert ist. Diebstahl kann durch biometrische Verfahren zur Aktivierung des Gerätes vorgebeut werden. Somit befreit ein leistungsfähiges Mobilgerät den Träger von der Notwendigkeit, sich immer wieder neu bei einem Terminal einzuloggen.

Ist diese Funktion der Authentifikation gegeben, kann auch die Verwendung von Zahlungsmitteln über das Gerät

als „physikalisches Wallet“ abgewickelt werden. Damit sind für den B2C-Bereich erheblich bessere Voraussetzungen geschaffen als heute, da das physikalische Wallet jederzeit eine Kommunikation auf Basis ausgewählter Sicherheitsparametern des Besitzers realisiert. Wenn gefordert, werden zwischen dem Gerät und der Außenwelt nur verschlüsselte, signierte und quitierte Nachrichten ausgetauscht. Die heute noch schwierige Handhabung dieser Mechanismen bleiben hinter einer einfachen Benutzerschnittstelle verborgen.

Bandbreiten

Die Multimedia-Fähigkeit eines Festnetzanschlusses erlaubt einen beliebigen Wechsel zwischen Anwendungen und Personen. Während die meisten Privatpersonen heute noch nicht über den „CallMe-Button“ mangels Leitungen oder Bandbreite eine zusätzliche Telefonverbindung aufbauen können, ist dies angesichts der xDSL-Technologie unproblematisch. Auch Konferenzschaltungen könnten zumindest im Bereich des B2B-Commerce zum Dauerzustand werden. Folglich ist zu erwarten, daß bis zum Jahre 2010 eine weitere Facette des Electronic Commerce in der multimedialen Unterstützung von Geschäftskommunikation zwischen Personen entstehen wird. Virtuelle Treffen, Verhandlungen, Projektbesprechungen etc. lassen sich bei erheblich niedrigeren Kosten durchführen. Experten lassen sich „auf Knopfdruck“ konsultieren und der Makler in Spanien kann dem Interessenten mit der Videokamera einen ersten Eindruck der Immobilie verschaffen.

Fernsehen als handelbares Gut

Heute wird beim Fernsehen in großen Zahlen kalkuliert: Sender kaufen Filmkontingente bei Filmhändlern für Milliardenbeträge ein, die dann im Laufe eines Jahres ausgestrahlt werden. Fernsehkanäle werden en-bloc von Rundfunksendern angemietet und Werbetreibende zahlen 50.000 Euro für die Ausstrahlung einzelner Werbespots, die dann wiederum Millionen Zuschauer ansehen.

Wie bereits anfangs erwähnt, liegt einer der Haupteffekte des Electronic Commerce in der Atomisierung des Geschäftslebens. Im Rundfunkbereich bedeutet dies:

- Adressierbarkeit der einzelnen Person (nicht nur des einzelnen Anschlusses!)
- Personalisierung des Angebotes gemäß einem Nachfrageprofil
- Eingriff des einzelnen „Zuschauers“ als Akteur
- Herunterbrechen von Kontingenten (Satellitenkanäle, Inhalte, Werbung)

Denkbar sind folglich elektronische Marktplätze für Fernsehsendungen. Hierbei rotten sich tausende oder vielleicht hunderttausende von Fernsehzuschauern zusammen und bilden eine virtuelle Einkaufsgemeinschaft. Jeder teilt dem Broker-System mit, zu welchem Preis er sich für welchen Film interessiert. Wenn für die Angebotsseite eine kritische Masse erreicht ist, übernimmt einer der Anbieter das Kontingent (natürlich in der Hoffnung, daß sich anschließend noch weitere Zuschauer registrieren). Video-on-Demand gewinnt damit den Charakter einer holländischen Auktion: der Preis wird (in Form der Gesamtnachfrage) solange erhöht, bis der erste Anbieter „zugreift“. Alle anderen Anbieter müssen sich nun nach einem anderen Kontingent umsehen. Nach dieser Informations- und Verhandlungsphase tritt das System zum Sendezeitpunkt in die Abwicklung ein, dabei können Techniken genutzt werden, die bereits heute zur Verfügung stehen, etwa die Schlüsselverteilung á la D-Box und die Ausstrahlung á la DVB.

Ökonomisch betrachtet, wird die drastische Kostenreduktion von Bandbreite zur weiteren Atomisierung des Fernsehbetriebs führen – von der Produktion über die Programmplanung bis zur Ausstrahlung. Kleine Nischenanbieter können sich gegenüber großen Sendern emanzipieren. Gleichzeitig wird Fernsehen zu einem aktiven Auswahlprozeß, da sich die Anzahl der Sender drastisch erhöht. Im Bereich der elektronischen Programmauswahl werden somit zunehmend Mechanismen wie Suchmaschinen und Verzeichnisdienste erforderlich, die bereits heute zur Navigation im Internet genutzt werden.

6.2 Online-Kataloge

Der Online-Katalog, auch *elektronischer Produktkatalog* genannt, stellt im chronologischen Verlauf der Handelstransaktion die erste Schnittstelle eines Unternehmens zum Markt dar. Der Katalog wird vom Kunden genutzt, um sich über das Produktangebot zu informieren sowie über Preis- und Lieferkonditionen etc.

Ein Katalog ist normalerweise nach Kategorien strukturiert und stellt dem Anbieter Werkzeuge zur Definition der Katalogstruktur, der Produktinformationsseiten sowie des grafischen Layouts zur Verfügung. Katalogseiten sind damit hochdynamische Web-Inhalte, da die Ebenen der *Präsentation* (Layout), der *Datenmodellierung* (Katalogstruktur und Produktattribute) und der *Inhalte* (Produktinformationen) frei vom Anwender definiert werden können. Kataloge sind daher nicht nur bez. ihres grafischen Datsellung sondern auch hinsichtlich ihrer Administrationsschnittstelle stark strukturiert.

Kataloge erfordern auf allen Ebenen eine permanente Pflege. Da häufig mehrere tausend Artikel auf dem aktuellen Stand zu halten sind, ist neben der manuellen Aktualisierung auch der Austausch von Daten mit anderen Softwaresystem erforderlich. Hierbei werden beispielsweise Produktdaten aus der Artikeldatenbank des Unternehmens extrahiert. Gleiches gilt für Preise und Lagerbestände. Ein Online-Katalog sollte direkt mit der Warenwirtschaft des Unternehmens integriert sei, damit jederzeit für den Kunden erkennbar ist, ob ausreichend Ware für seine Bestellung am Lager ist und damit gleichzeitig das Auslieferungslager informiert werden kann, wenn ein Kunde online eine Bestellung aufgegeben hat.

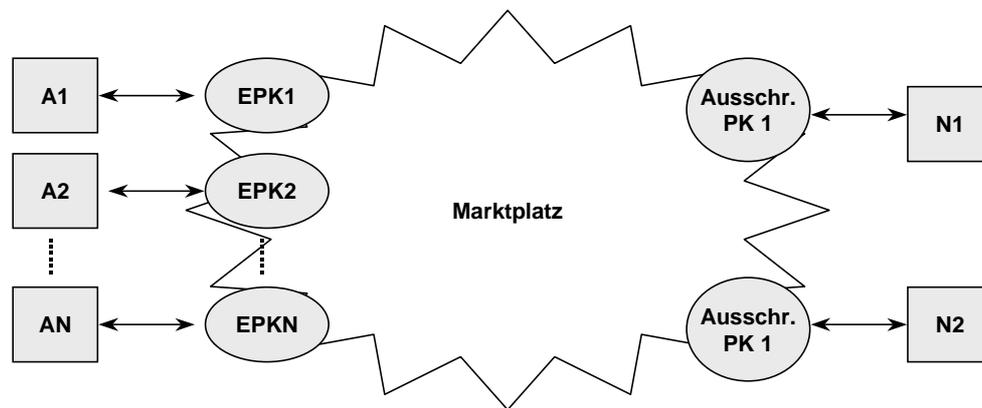


Abb. 19: Anbieter- und Nachfragerkataloge auf dem elektronischen Markt

Abb. XXX3 zeigt schematisch, wie sich heute isolierte Kataloge der Anbieter und Nachfrager auf dem elektronischen Marktplatz gegenüber stehen. Ein Nachfragerkatalog ist dabei ähnlich organisiert wie der eines Anbieters, nur mit dem Unterschied, daß nachgefragte Artikel veröffentlicht werden. Diese können bereits mit einem Preis versehen sein, so daß Anbieter nur noch die Wahl der Zustimmung oder Ablehnung des spezifizierten Kontrakts haben oder die Inhalte des Katalogs können als Ausschreibung aufgefaßt werden, gegen die mehrere Anbieter mit ihren Konditionen bieten können.

Bis auf wenige Branchen wie etwa die Tourismusindustrie mit ihren Reservierungssystemen ist der Markt heute gekennzeichnet durch herstellereigene Kataloge. Dies führt zu einer Vielzahl heterogener Online-Shops, die sich jeweils durch unterschiedliche Angebotstaxonomien, Bezeichnungen Datentypen und Web-Schnittstellen unterscheiden. Diese Individualität erlaubt zum einen die Darstellung des eigenen Angebots nach individuellen technischen Maßgaben und der Corporate Identity des Unternehmens. Zum anderen erschwert diese Intransparenz gleichzeitig den direkten Vergleich konkurrierender Angebote. Diese Intransparenz gilt sowohl für Kunden als auch für Software-Agenten, die zwar effizienter Preise vergleichen können, die jedoch nur bei einer homogenen Repräsentation der Produkte.

Für die nächsten Jahre ist jedoch zu erwarten [ScZi97], daß aufgrund der vorne erwähnten „Commoditization“ die Spezifikation für Standardprodukte vereinheitlicht wird. Dies kann dann zur Dominanz neutraler Kataloge führen, die nicht einfach nur auf die unterschiedlichen Web-Angebote der Hersteller verweisen (wie heute etwa Yahoo oder Web.de), sondern über eine Anbieter-Schnittstelle den Upload einzelner Angebote zulassen.

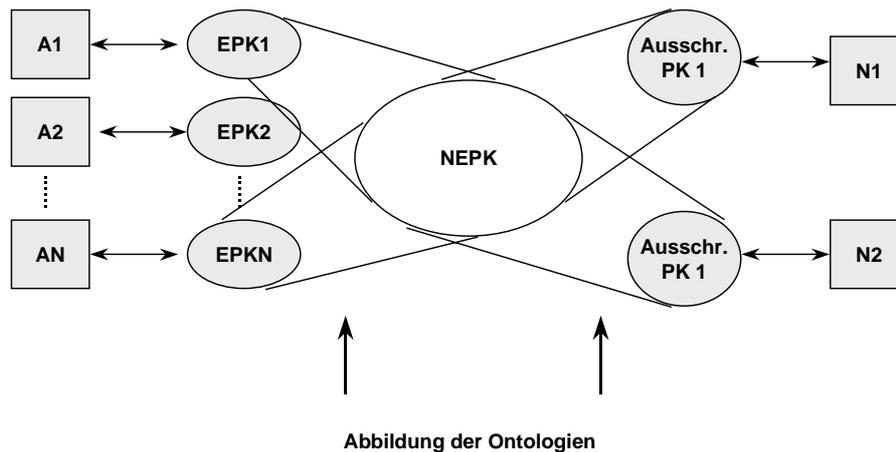


Abb. 20: Die Rolle des neutralen elektronischen Produktkatalogs

Eine einheitliche Referenzausstattung des VW-Golf würde dann beispielsweise über den Preis der vertretenen Händler sortierbar sein. Derart integrierte Produktkataloge sind jedoch nicht kurzfristig für beliebige Produkte zu erwarten, da hier die wesentliche Hürde im Integrationsaufwand der Angebote liegt: Entweder ist eine N:1-Konvertierung der verschiedenen Anbieter zur Darstellung des Katalog erforderlich oder die Anbieter standardisieren eine einheitliche Darstellung, die sie jeweils intern verwenden. Die Abbildung der jeweiligen Vokabulare bzw. Ontologien dürfte hierbei jedoch das größte Problem darstellen. Solche Standardisierungsprozesse können Jahre erfordern, wie die Erfahrungen im Bereich des elektronischen Datenaustausches zeigen (vgl. Abschnitt XXX zum Thema EDI).

XXX EDI-Katalog hierher???

6.2.1 Ein Beispiel

1. Der Linotype FontExplorer@Web.

Das Unternehmen Linotype® bietet auf dem internationalen Markt hochwertige Schriften für den Gebrauch auf PCs und Macintoshs an. Dabei steht insgesamt eine Palette von ca. 30.000 Schriften zur Verfügung von denen bisher nur 5.000 per CD-ROM an die Kunden ausgeliefert wurden. Dabei dient der FontExplorer®, der zusammen mit der CD-ROM ausgeliefert wird, als Retrieval-Werkzeug zur Ermittlung der gewünschten Schrifttype.

Schriften lassen sich nach für den Laien mehr oder weniger offensichtlichen Kriterien klassifizieren: Bezüglich der Schriftmetrik lassen sich Serifenschriften von serifenlosen unterscheiden. Schriften können ferner nach ihrer Eignung für die Anwendungsbereiche Buchdruck, Zeitschriften, Anzeige bzw. Web-Seiten eingesetzt werden. Weitere Kriterien sind zum Beispiel die Serifenform, die historische Einordnung der Schrift bis hin zur eher emotionalen Anmutung der Schrift. Hier stehen Klassifikationen in Bereichen wie „ordinär—exklusiv“ oder „männlich—weiblich“ zur Verfügung.

Alle 30.000 Schriften lassen sich nun mit derartigen Attributen klassifizieren, wobei keine nennenswerten Abhängigkeiten zwischen ihnen bestehen. Damit sind alle Attribute in beliebiger Kombination für die Selektion aus dem Produktkatalog einsetzbar, was dem Kunden eine hochflexible Möglichkeit bietet, durch sukzessives Festlegen der gewünschten Kriterien, die Menge der passenden Schriften von einigen tausend auf beliebig wenige einzuengen.

Ein Standard-Katalog, wie er bei den meisten Shop-Systemen angeboten wird, würde hier nicht weiterhelfen, da das Auf- und Abnavigieren in der Kataloghierarchie nicht der Unabhängigkeit der Attribute gerecht werden würde – es können keine beliebigen, vom Kunden festgelegten Suchkriterien angewendet werden. Auch die Integration einer Suchmaschine würde nicht weiterhelfen, da die Ausprägungen einiger Attribute nur numerisch vorliegen. Schließlich würde das Navigieren durch den hierarchischen Katalog viel zu lange dauern, wenn neben der eigentlichen Attribut- und Produktinformation auch noch die komplette HTML-Seite geliefert werden müsste.

Folglich wurde für den FontExplorer@Web ein eigener Ansatz gewählt, der durch die Unterstützung eines Applets, die Festlegung der Suchattribute radikal vereinfacht und gleichzeitig das Laden der Produktinformationen in kürzester Zeit erlaubt.

Diese hohe Ergonomie und Effizienz bei der Navigation im Katalog ist eines der kritischen Erfolgsfaktoren bei der Einführung eines Online-Katalogs. Weitere Informationen zu diesem Projekt sind unter XXX Ponton-Lino-Presserklärung] zu finden. Abb. XXX zeigt eine Bildschirmaufnahme der Benutzerschnittstelle des Linoty-Katalogs.

XXX Screen-Shot hierher!

Abb. XXX: Der ForntExplorer@Web von Linotype

6.3 Profile und abgeleitete Daten

6.3.1 Warum Profile?

Profilinformation bezieht sich auf Eigenschaften, Präferenzen oder Verhaltensweisen eines Teilnehmers, die entweder von ihm selbst definiert und damit in einheitlicher Form anderen bewußt zur Verfügung gestellt werden sollte oder als Ergebnis von Sitzungsprotokollen. Profile lassen sich ebenso für Angebote, Ressourcen oder die Fähigkeiten und Erfahrungen eines CallCenter-Agent definieren.

Profile sind neben der Abrechenbarkeit von Online-Käufen eine weitere grundlegende Technologie, die ein Online-Anbieter beherrschen muß, wenn er das Automatisierungspotential eines Online-Shops nutzen will.

Auch auf der Kundenseite helfen Profile, redundante Interaktionen zur Dateneingabe zu vermeiden: Wenn sich ein Teilnehmer bei einem Dienst registrieren läßt, werden immer wieder die gleichen Daten abgefragt - Name, Adresse, e-Mail etc. Profile können hierbei helfen, diese Information in standardisierter Weise zu übertragen, so daß das Ausfüllen endloser Formulare vermieden werden kann.

Unabhängig von der Festlegung von Profilinformationen, geht es jedoch beim Datenschutz um die Vermeidung einer mißbräuchlichen Verarbeitung dieser Information. Dieses Kundeninteresse steht jedoch der des Online-Anbieters diametral gegenüber: für ihn stellt Profilinformation eine wertvolle Quelle der Markt- und Kundeninformation dar. Sowohl das Verhalten und die Präferenzen eines jeden Einzelnen als auch die der aggregierten Gesamtnachfrage kann mit bisher unerreichter Präzision gemessen werden. Eine Marktanalyse konnte ohne das WWW bisher nur von vagen Annahmen hinsichtlich der Wahrnehmung und des Interesses der Konsumenten ausgehen. Mit dem Online-Profiling steht hingegen ein Instrument zur Verfügung, das in seiner Präzision weit über statistische Methoden hinausgeht.

Online-Profiling liefert u.a. folgende Informationen:

Informationen zur zeitlichen Verteilung der Nutzung eines Online-Angebotes im 24-Stunden- oder Wochenrhythmus.

- Informationen aus Besuchsdaten
- Informationen aus Kommunikationsaktivitäten
- Transaktionsdaten

Zudem kann Profilinformation klassifiziert werden nach der Qualität der anfallenden Daten. In dieser Dimension unterscheidet man

- **Anonyme Daten.** Unter diese Kategorie fallen alle Informationen die aus dem Bewegungsprofil der Benutzer abgeleitet werden können, ohne deren Identität zu kennen,
- **Kundendaten mit niedriger Verbindlichkeit.** Hierbei gibt sich der Benutzer zu erkennen, indem er ein Formular ausfüllt oder eine E-Mail sendet. Mangels Zertifikate besteht hierbei jedoch keine Möglichkeit, die Aussagen des Benutzers zu authentifizieren. Damit haben diese Informationen niedrigere Qualität als
- **Kundendaten mit hoher Verbindlichkeit.** Diesen Daten liegt eine Authentisierung zugrunde, die unmittelbar ihre Präzision und Zurechenbarkeit erhöht. Wenn ein Kunde sich für einen Kauf entschließt und dafür seine Kreditkarte einsetzt, bedeutet dies erstens, daß er nicht nur Interesse am Produkt bekundet, sondern dieses auch in einen Online-Kauf umsetzt.

Transaktionsdaten eignen sich folglich zur Modellierung des individuellen Kunden, so daß ihm eine Umgebung bereitgestellt werden kann, die seinen Präferenzen entgegenkommt, z.B. indem individuell passende Angebote

einblendet werden. Transaktionsdaten fallen im Vergleich zu anonymen Daten in weitaus geringerem Volumen an, jedoch bei erheblich höherer Präzision.

Umgekehrt eignen sich anonyme Daten eher zur abstrakteren Marktanalyse und damit zur Modifikation des Gesamtangebotes eines Online-Shops.

Beide Formen von Profildaten lassen sich für den Betreiber in unterschiedlicher Weise kommerzialisieren: Während Transaktionsdaten eher den Adressenlisten entsprechen, die einschlägige Händler an Versicherungen, Banken oder andere Interessenten vermitteln, geht es bei anonymen Daten eher um Marktanalysen, wie sie heute nur mit sehr hohem Aufwand von spezialisierten Unternehmen wie etwa Nielsen, Forrester Research oder Ovum angeboten werden.

Marktdaten lassen sich aus den kombinierten Profilinformatoren mehrerer Anbieter destillieren; dazu ist es jedoch erforderlich, die zugrunde liegende Information zu standardisieren.

Abb. XXX zeigt den Zusammenhang zwischen dem Grad an Anonymität und der Qualität der Profildaten auf:

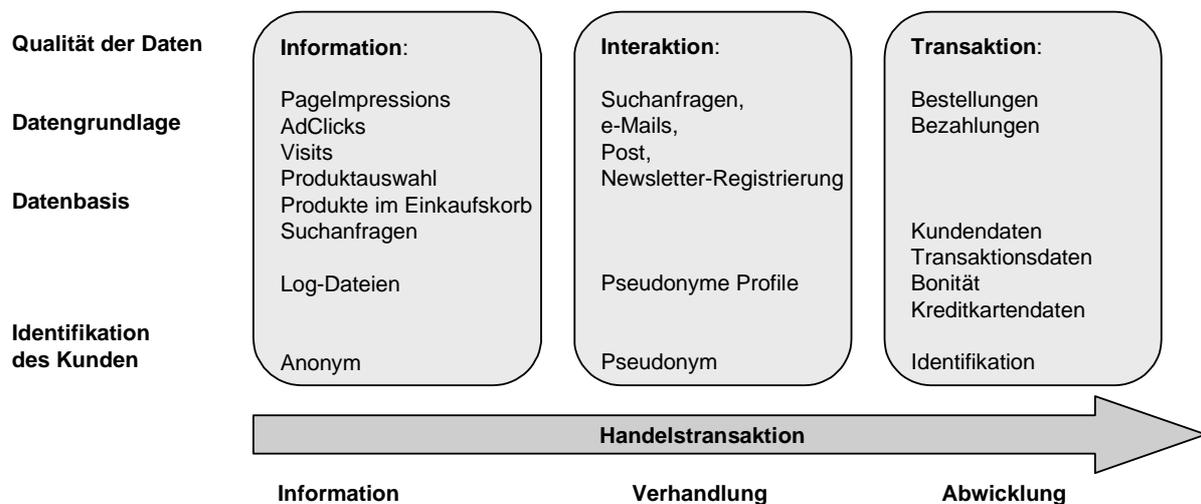


Abb. 21: Qualität und Anonymität von Benutzerprofilen

Ein Online-Anbieter verfolgt mit Profilen folgendes Interesse:

- Präzisere Platzierung von Werbebannern.
- Zur Anbieterplattform zugeschaltete Content-Provider können besser unterstützt werden in einer effizienteren Organisation ihrer Inhalte.
- Langwierige Registrierungsprozeduren lassen sich effizienter gestalten.
- Probleme mit Cookies können umgangen werden (siehe unten).

Mit Hilfe standardisierter Profilinformatoren auf der Basis von OPS oder P3P (s.u.) besteht zusätzlich die Möglichkeit, auf aufwendige Analyse und Bewertungsprozeduren zu verzichten, da das erforderliche Instrumentarium ebenfalls als Standardprodukt erworben werden kann. Content-Providern eines Online-Dienstes steht damit ein verlässlicherer Analysemechanismus zur Verfügung als es bei Cookies oder der Beobachtung des IP-Verkehrs der Fall wäre.

6.3.2 Cookie-Information

Die im folgenden erörterten Mechanismen erläutern Möglichkeiten, wie der Betreiber eines Web-Servers Informationen über den Kunden erlangen und diese Informationen seitens des Kunden-Browsers speichern kann.

Der „Referer-Link“

Informationen aus dem GET-Befehl schließen u.a. die URL der aktuellen Seite ein. Dies hilft, Zusammenhänge zwischen einzelnen Web-Zugriffen zu ermitteln und Navigationsprofile zu erstellen. Dies kommt insbesondere

der Erstellung von Pfad-Profilen zugute, welche helfen, den Navigationspfad eines Benutzers nachzuvollziehen.

Cookies

Mit dem Navigator 2.0 führte Netscape die Spezifikation der Cookies ein. Ursprüngliche Aufgabe der Cookies war die Protokollierung von Web-Zugriffen eines Benutzers. Insbesondere für Shopping-Anwendungen bieten sich Cookies an, da sie durch die Definition einer Session-ID als Bestandteil des Cookies zustandsbehaftete Sitzungen realisieren helfen. Ein elektronischer Einkaufswagen kann dabei dem Benutzer bei Übertragung der Session-ID dargestellt und aktualisiert werden.

Ein Cookie wird bei jedem HTTP-Befehl an den Server gesendet. Über serverseitige Programmierschnittstellen (oder CGI) wird der Cookie an nachgelagerte Server weitergereicht. Er kann damit auch von anwendungsspezifischen Erweiterungen des Web-Servers verarbeitet werden.

Cookies werden im Hauptspeicher des Browsers gehalten und - wenn sie persistent sind - in einer eigenen Datei gespeichert („cookies.txt“). Weitere Zustandsinformationen wie Farbpräferenzen oder präferierte Zahlungsmodalitäten können auf diese Weise für spätere Sessions wiederverwendet werden.

Cookies werden vom Web-Server an den Browser vor dem Text des HTML-Dokuments gesendet. „SetCookie“ definiert einen Cookie. Dabei werden Attribute als Listen von Name/Value-Paaren gesetzt. Beispiel für eine Set-Cookie-Message:

```
set-cookie:   lehrgebiete=chemie+physik+informatik;
              domain=.learning.de; path=/learning/;
```

Einige Attribute sind standardisiert:

```
Expires=<Zeit>
```

Spezifiziert den Zeitpunkt, zu dem der Cookie verfällt.

```
domain=...
```

Spezifiziert, zu welchen Rechnern (mit HTTP-Server) der Cookie gesendet wird. Normalerweise nur der, von dem er empfangen wurde.

```
path=...
```

Legt fest, welche Referenzen den Cookie auslösen. Wenn nicht spezifiziert, wird er bei allen HTTP-Zugriffen versendet. ansonsten nur an Seiten unterhalb des Pfades.

Mit Hilfe von Cookies können somit Benutzerprofile erstellt und gezielt personalisierte Werbe-Images eingestreut werden. Auch die Verzweigung zu den Werbeseiten kann verfolgt werden, so daß dem Werbe-Kunden eine detaillierte Zugriffsstatistik erstellt werden kann. Content-Providern beim Lerndienst kann auf diese Weise Information vermittelt werden, wer zu welchem Zeitpunkt welches Produkt gekauft hat.

Die Definition für Cookies (RFC 2109) legt jedoch fest, daß der Benutzer sie jederzeit ausschalten kann, um seine Anonymität zu wahren. Dieser Fall ist bei der Gestaltung der Billing-Lösung zu berücksichtigen.

6.3.3 Web-Tracking, Kundenprofile & Marktanalyse

Internet-Visitenkarten

Der Austausch persönlicher Daten erfolgt immer, wenn zwei oder mehr Personen kommunizieren – egal ob dies per e-Mail, per Telefon oder vis-a-vis erfolgt. Dabei werden immer wieder Adressen und andere Kontaktmöglichkeiten wie Telefonnummer oder Home-Pages ausgetauscht. Der Austausch dieser Daten erfolgt heute unstrukturiert, d.h., ohne Standardisierung von Syntax und Semantik dieser Daten. Daher ist es eine Bestrebung der Entwickler von Browsers und Internet-Werkzeugen, diese Information inoperabel zu machen, so daß sie bei Bedarf übergeben werden kann.

Der vCard-Standard wurde daher vom Internet Mail Consortium entwickelt, um diese Information – möglicherweise ergänzt um weitere Multimedia-Daten – zu standardisieren. VCard daten können Informationen über Personen oder Ressourcen beinhalten und als e-Mail-Attachment, per Datenaustausch oder als Datei im Verzeichnis übergeben werden. Zudem hilft ein solcher Standard, Medienbrüche zu vermeiden.

Management von Profilen

Ein einheitliches Management von Profilen der Nutzer und Anbieter von ADSL-basierten Diensten ist bereits aus administrativen Gründen im Hinblick auf die Authentisierung und Autorisierung von Teilnehmern erforderlich.

Durch die aktuell und zukünftig zusätzlich auftretenden regulatorischen Anforderungen des Gesetzgebers (siehe z.B. EU-Richtlinie EU95/64 zur Umsetzung von Datenschutzbestimmungen für den anbieterseitigen Umgang mit Profildaten) entstehen jedoch noch weiterreichende Anforderungen an das Profil-Management.

Herstellerspezifische Lösungen, wie sie derzeit beispielsweise von Routerherstellern für deren spezifische Belange realisiert und am Markt angeboten werden, bieten aufgrund konzeptioneller Unzulänglichkeiten keinen geeigneten Ansatz für die Erfüllung solcher Anforderungen.

Als Alternative bieten sich derzeit im Umfeld der Internet-Technologie mit hohem Tempo im Entstehen befindliche IETF- und Industriestandards zu netzgestützten Benutzerprofilen an.

6.3.4 Web-Marketing und Banner-Werbung

Noch vor zwei Jahren befürchteten viele Internet-Benutzer eine Werbeflut von Banner-Bitmaps, die die Bandbreite des Internet so stark belasten würde, daß das gesamte Medium in Frage gestellt wurde. Daß sich mit der wachsenden Nutzerzahl auch die Bandbreite der Backbones entsprechend erweitern konnte – mehr Benutzer finanzieren ja auch mehr Bandbreite – war nicht für jeden verständlich. Heute ist die Bitmap-Flut größer denn je, aber gleiches gilt auch für die Internetbandbreite im allgemeinen.

Mit der Banner-Werbung liegt nun eine ganze Industrie von beteiligten Unternehmen und Organisationen vor, die am neuen Werbemechanismus partizipiert:

Betreiber von Web-Servern wie Suchmaschinen, Shareware-Server, Informationsdienste etc. leben teilweise vollständig von den Werbeeinnahmen. Heerscharen von Designern versuchen, eine optimale Kombination aus Banner-Attraktivität und Dateigröße der Bitmap zu erzielen. Die werbetreibende Wirtschaft hat sich rasch auf Konventionen und Metriken geeinigt, um den Erfolg von Werbemaßnahmen messen zu können. Diverse neue Geschäftsideen sind als Randerscheinung der Banner-Werbung entstanden: *Click-Register* protokollieren als vertrauenswürdige Dritte die Anzahl der AdClicks, Eintragungsdienste helfen dem Newcomer bei der Registrierung seiner Web-Site bei den wichtigsten internationalen Suchmaschinen. Schließlich betreiben weitere Unternehmen (häufig als Einzelkämpfer) sogenannte Banner-Tauschprogramme, mit deren Hilfe sich eine Vielzahl an Web-Sites gegenseitig in der Erlangung von Aufmerksamkeit stützen können.

Meßverfahren des IVW

Der IVW (XXX I... V... W...) dient als neutrale Meßinstanz, die für freiwillig registrierte Online-Anbieter eine monatliche Zugriffsstatistik veröffentlicht. Diese Informationen werden regelmäßig unter der Web-Adresse www.ivw.de/XXX zur Verfügung gestellt. Die wichtigsten Meßkriterien sind dabei die PageImpressions und die Visits:

- *PageImpressions*. Diese Kennzahl gibt an, wie häufig Web-Seiten vom Server abgerufen wurden. Dabei muß sie unabhängig sein von der Seitengestaltung, insbesondere von der Anzahl der Frames und Bitmaps, da diese jeweils einen Hit beim Web-Server – also einen Eintrag in seiner Protokolldatei – verursachen. Aus diesem Grunde werden nur Abrufe der tatsächlichen HTML-Seiten gezählt. PageImpressions können dennoch nur in Grenzen die tatsächlichen Abrufe reflektieren, das es von geschachtelten Frames sowie der Kombination aus statischen und dynamischen Bestandteilen einer Seite abhängt, wie oft und lange beispielsweise ein Werbebanner für den Kunden sichtbar ist.
- *Visits* sind Besuche bzw. Nutzungsvorgänge. Immer wenn ein Benutzer von einem anderen Web-Server auf den betreffenden wechselt, wird dieser Einstieg als ein Visit protokolliert. Besucher können über ihre Visits hinaus nicht weiter unterschieden werden, da der Zugriff anonym erfolgt. Somit ist nicht meßbar wie oft ein einzelner Benutzer einen Web-Server besucht, bzw. wie groß der „Leserkreis“ eines Web-Servers ist.

Schaut man sich die Statistik des IVW an (vgl. Abb. XXX), so stellt man fest, daß pro Visit nur durchschnittlich 3-5 PageImpressions erfolgen. Dies zeigt in beeindruckender Weise, wie schnelllebig ein Besuch beim Server ist.

XXX IVW-Statistik März 99 hier einfügen!!!

XXX Statistik kommentieren.

6.3.5 Explizite Teilnehmerprofile

Explizite Teilnehmerprofile werden vom Benutzer bewußt bereitgestellt. Diese Information hilft, wiederholten Konfigurationsaufwand zu vermeiden und nur in Ausnahmesituationen den Benutzer zu involvieren. Derartige Teilnehmerprofile beziehen sich auf folgende Informationen:

- **Persönliche Daten.** Hierbei handelt es sich um Adressinformation, Kontaktinformation im Internet, Angaben zur Person (Geschlecht, Alter, etc.).
- **Sicherheitsprofile.** Bei dieser Art von Profilen definiert ein Teilnehmer Sicherheitskomponenten, die er für die Kommunikation als erforderlich erachtet. Dabei stehen vor allem Anforderungen der Verschlüsselung, der Nachrichten- und Benutzerauthentisierung, der Integrität sowie der Nichtabstreitbarkeit im Vordergrund.
- **Präferenzen.** Diese Profilverinformation ist weniger standardisierbar, sie hängt zumeist vom Angebot eines Online-Dienstes ab. Präferenzen umfassen dabei Interessengebiete, die sich durch die Auswahl von Informationskanälen, Nachrichtentypen, Literatur etc. niederschlagen.
- **Kommunikationsparameter.** Auch die Konfiguration einer Kommunikationsverbindung (wie z.B. die Bandbreite bei ADSL upstream/downstream) wird als Teil des Benutzerprofils verwaltet.

Voraussetzung für explizite Profile ist das Ausfüllen von Online-Formularen.

6.3.6 Abgeleitete Profile

Abgeleitete Profile entstehen ohne ausdrückliche Bereitstellung durch den Teilnehmer. Sie fallen an aufgrund der getroffenen Seitenauswahl, der getätigten Online-Käufe oder aus der Kombination solcher Informationen von unterschiedlichen Benutzern. Beispiele für derartige Informationen sind:

- **Sitzungsdauer.** Hierbei wird gemessen, wie lange ein Teilnehmer welche Information einseh.
- **Transaktionsdaten.** Kaufinformationen (Artikel, Anzahl, Uhrzeit, Kundendaten etc.) werden nur beim Abschluß eines Online-Geschäfts anfallen. Sie haben allerdings die höchste Ausdrucksfähigkeit bzw. Qualität.
- Produkte, die in **elektronische Einkaufskörbe** gelegt wurden. Auch hier unterstützen Online-Shopping-Systeme persistente Einkaufskörbe, die es erlauben, auch anonyme Teilnehmer bez. ihrer Produktauswahl zu verfolgen. Im Gegensatz zu angesehenen Katalogeinträgen, haben in den Einkaufskorb gelegte Artikel höhere Aussagequalität über Kundenpräferenzen.
- **Produktauswahl und -kombination.** Neben seinem Inhalt ist auch die Kombination von Produkten im Warenkorb interessant für das Bündeln von Warenangeboten. So können häufig nachgefragte Kombinationen prominent auf einer Portalseite plaziert oder ein entsprechender Auszug aus dem Online-Angebot als Paket angeboten werden.
- **PageImpressions.** Hierbei wird erfaßt, wie oft welche Web-Seiten angesehen wurden. Bewegungsprofile lassen sich zwischen den Seiten eines einzelnen Anbieters, aber auch zwischen mehreren Servern feststellen – zumindest woher der Teilnehmer kam.
- **AdClicks.** Hierbei wird gezählt, wie oft eine Banner-Werbung vom Benutzer angeklickt wurde. Diese Information ist relevant für die Abrechnung von Banner-Werbung, da dies häufig (neben einem Fixum) nachfragebasiert erfolgt.
- **Automatische Anfragen, Queries.** Häufig wird eine Kataloganfrage anhand von Einträgen in Web-Formulare vom Web-Server generiert, so daß häufige Anfrageausdrücke erkannt werden können und, statt einer erneuten Auswertung, das Ergebnis bereits aus dem Cache geliefert werden kann. Suchmaschinen verwalten intern semantische Netze, um Anfragen für Volltextrecherchen nicht nur bez. des Suchbegriffes, sondern auch nach sematisch "benachbarten" Begriffen durchzuführen.

6.3.7 Verdichtete Profilinformatio

Schließlich kann detaillierte Profilinformatio zu aggregierten Aussagen verdichtet werden. Dies hilft, Nutzungsstatistiken zu erstellen, Muster zu erkennen und Zusammenhänge herauszufiltern, die sich erst anhand einer hinreichend großen Grundgesamtheit an Daten ermitteln läßt. OLAP- und Data-Mining-Werkzeuge dienen hier zur Automatisierung eines solchen Vorgehens.

1:1-Marketing

Niemals in der Vorweb-Ära bestand für ein Unternehmen die Chance, einen Kunden individuell zu adressieren: Es wurde das Publikum der Massenmedien mit Werbespots „mit der Gießkanne“ berieselt, ohne wirklich zuverlässige Informationen über deren Aufmerksamkeit beim Empfänger zu erlangen. In den gängigen Medien werden 30-Sekunden-Slots zu astronomischen Preisen müssen erworben (XXX → Preise nachschlagen). Für den Preis eines einzigen 30-Sekunden-Werbespot zur PrimeTime bei RTL kann sich ein Unternehmen heute einen 512 Kbit-Internet-Zugang leisten. Wenn es auch noch das Budget für wenige weitere Spots gegen die Entwicklung einer attraktiven Homepage mit Banner-Werbung und Customer-Profiling eintauscht, adressiert es nicht nur eine weltweite Klientel, sondern verfügt auch über hochpräzise Information über diese Kunden. Einige Unternehmen beginnen bereits, diese Profilinformatio zu kommerzialisieren, indem sie Statistiken, verdichtete Daten oder den Zugang zu ihrer Profildatenbank Dritten anbieten.

Eine wichtige Voraussetzung für die individuelle Ansprache des einzelnen Kunden durch Banner-Werbung liegt in den Mechanismen zur Erstellung, Verwaltung und Anwendung von Kundenprofilen. Denn nur, wenn Daten über seine

- Personalisierung
- Activity Tracking, Referer-Link
- Bewegungsprofile
- Kaufprofile

Profilerstellung zur:

- Mustererkennung
- Ermittlung des Web-Verhalten (XXX-Index)
- Seiten-/ Produkt-Kombinationen
- Trefferraten von HTML-Seiten und Anzeigen
- Statistik-Auswertung

Neben diesen Daten, die allein vom Web-Server stammen, lassen sich weitere Informationen berücksichtigen wie z.B. Bonitätsinformationen, Online-Telefonverzeichnisse, oder auch demographische und geographische Statistiken zum Einkommensniveau etc.

6.3.8 Data Warehouses

Aufgrund der überwältigen Flut an Daten, die durch Profilinformatio und Online-Transaktionen anfallen, sind es heute nicht nur Großunternehmen wie Fluggesellschaften oder Handelshäuser, die an Kunden- und Nachfrageprofilen interessiert sind, sondern jeder Anbieter von Online-Information.

Data-Warehousing ist ein Verfahren, große Datenmengen so zu organisieren, daß sie in integrierter, sachbezogener und einfach analysierbarer Form vorliegen. Ein Data-Warehouse – das sich am besten mit „Datenlager“ übersetzen läßt – wird in regelmäßigen Abständen vollständig aktualisiert und dazwischen nur für lesende Zugriffe genutzt. Das Data-Warehouse unterstützt Entscheidungsträger bei der Verdichtung der Rohdaten zu aussagekräftigen Kennzahlen. Hierzu werden üblicherweise Zeitreiheninformationen, nach geographischen oder organisatorischen Kriterien verdichtete Informationen oder auch Informationen unterschiedlicher Verdichtungsstufen verwaltet. Da diese Datenkategorien jeweils unabhängig sind, kann man sich das Data-Warehouse als einen mehrdimensionalen Würfel vorstellen, den man aus unterschiedlichen Perspektiven zerlegen kann. Der sogenannte „Drill-Down“ stellt dabei einen Abstieg von hochverdichteten Kennzahlen bis hin zu operativen Rohdaten dar. Durch die „Würfelform“ ist das Datenvolumen erheblich höher als die redundanzärmere Repräsentation von Unternehmensdaten in normalisierter Form. Das Optimierungsziel dieser Organisation liegt folglich in einer effizien-

enten Unterstützung von Analyseabfragen.

Online Analytical Processing

Der Begriff des Online Analytical Processing (OLAP) steht dabei für die technische Unterstützung dieses Analysevorgangs. Eine besondere Herausforderung des OLAP liegt in der Kombination von strukturierten und nicht-strukturierten Daten. Hier können in einem größeren Unternehmen unterschiedliche Kodierungen, Datenmodelle und Kommunikationsprotokolle vorliegen, die zur Gewinnung eines konsistenten Warehouses zu vereinheitlichen sind. Die Rohdaten müssen daher ermittelt, bereinigt, zentralisiert und umorganisiert werden, bevor sie in das Data-Warehouse einfließen:

- *Datenermittlung* (data acquisition). Dieser Prozeß setzt die Schaffung eines einheitlichen Zugriffsprotokolls voraus, wie es z.B. durch ODBC oder JDBC im Falle relationaler Datenbanken gegeben ist. Falls Daten semi-strukturiert vorliegen (z.B. als XML-Dokumente), ist ein entsprechender Transformationsprozess erforderlich.
- *Datenbereinigung*. Hierbei werden mehrere Verfahren unterschieden: Zunächst sind redundante Bezeichnungen zu vereinheitlichen. Dabei kann es z.B. vorkommen, daß gleiche Artikel in internationalen Filialen unterschiedlich benannt werden. Gleiches gilt für Preise unterschiedlicher Währungen oder uneinheitlicher Wechselkurse. Hier ist die Transformation in eine einheitliche Bezeichnung nötig. Buchungen können doppelt vorliegen, insbesondere, wenn Stornierungen sich von regulären Buchungen nur durch eine besondere Kennung unterscheiden. Außerdem kann die Integrität der Daten verletzt werden, wenn entsprechende Umbenennungen bei der Datenbereinigung erfolgen. Aus diesem Grunde bieten Hersteller Werkzeuge an mit deren Hilfe, der Ausgangs- und der Zielzustand der Daten modelliert und somit die Transformationsfunktion automatisch generiert werden kann. Monitoring-Systeme sind dabei innerhalb enger Grenzen in der Lage, diesen Prozeß zu überwachen und „verdächtige“ Konstellationen zu melden. Soche Systeme stehen z.B. von den Anbietern *Trillum* und *Integrity* zur Verfügung.
- *Daten laden und aktualisieren*. Die Übernahme der Daten in das Data-Warehouse erfordert weitere Schritte der Verarbeitung wie Integritätschecks, Sortierungen, Neunumerierungen, Aggregationen, Partitionierungen und die Erstellung von Indexinformationen.

Ist das Data-Warehouse einmal mit „sinnvollen“ Daten gefüllt, gilt es im nächsten Schritt, ihm sinnvolle Informationen zu entlocken. Dies erfolgt durch den sog. „Drill-Down“ nach unterschiedlichen Verfahren:

- Der *Roll-Up* liefert eine Aggregation innerhalb einer oder mehrerer ausgewählter Dimensionen. So können etwa Tagesumsätze zu Quartalsumsätzen verdichtet werden oder einzelne Filialen zu Regionen.
- Beim *Slicing* geht die Analyse vom Schnitt entlang einer Dimension des Würfels aus: Wie setzt sich der Umsatz aller Filialen bzgl. aller Produkte am 30.6.1999 zusammen? Hierbei wurde der Würfel quer zur Zeitachse zerschnitten. Informix nennt Add-On-Funktionen zur Datenanalyse folglich auch „Datenklingen“ (*Data Blades*). Das *Slicing* kann unabhängig von der Dimension durchgeführt werden, so daß sich der Anwender schrittweise an Details herantasten kann.
- Das *Dicing* erlaubt im Gegensatz zum *Slicing* die Definition von Bereichen, so daß als Resultat ein Sub-Würfel geliefert wird.
- Schließlich erlauben *Pivot-Tabellen* (bzw. das *Pivoting*) eine selektive Aggregation entlang mehrerer Dimensionen.

Dieses Analyseverfahren lassen sich in unterschiedlicher Form durch die Datenbank unterstützen:

- Beim *MOLAP* (*Multidimensional OLAP*) liegt für jeden potentiellen Wert, der sich aus den Schnittpunkten der multidimensionalen Ausprägungen in der Datenbank ergibt, tatsächlich ein Speicherplatz vor. Dieser muß jedoch nicht notwendigerweise immer durch einen gültigen Wert belegt sein. Folglich kann die Gesamtgröße der Datenbank häufig auf mehrere Terabyte ansteigen. Andererseits werden Abfragen entsprechend schnell beantwortet.
- Beim *ROLAP* (*Relational OLAP*) werden die operativen Daten in einer Rohdatentabelle (fact table) belassen und um eine Dimensionstabelle ergänzt. Diese enthält Meta- und Aggregationsinformationen (Produktinformationen, Geographische Lokationen).

Angewendet auf Profilinformatoren lassen sich nun Data-Mining-Verfahren anwenden, mit deren Hilfe nach unterschiedlichen Dimensionen Kunden-, Transaktions- und Produktprofile analysiert werden können. Per Data Mining kann z.B. ein Unternehmen feststellen, welche Kundengruppen in welcher Region zur einer bestimmten

Uhrzeit Bücher kaufen.

Ein Online-Angebot kann in entsprechender Weise konfiguriert werden, so daß Angebote für Produkte, deren Profil „paßt“, den ermittelten Kunden auf ihre Portalseite projiziert werden können.

Recommendation Engines

Produkttempfehlungen, die auf der Web-Seite des Kunden erscheinen sollen sind besonders volatil – sie hängen ab von Kunden- und Produktprofil, von der Historie bisher gekaufter oder betrachteter Produkte, sowie von allgemeinen Vorlieben für bestimmte Produktkombinationen, die sich aus der Masse von Visits und PageImpressions ergeben haben. Diese Informationen lassen sich nicht mehr manuell durch Mitarbeiter auswerten und in entsprechende Konfigurationen von Web-Seiten umsetzen. Zur Bewältigung dieser Komplexität werden heute ebenfalls Produkte angeboten, die automatisch auf den genannten Input-Informationen in Echtzeit oder über mehrstufige Analyseschritte die „semantische Nähe“ zwischen Produkten ermitteln.

Eines der ersten und berühmtesten Beispiele ist (mal wieder ;-) Amazon.Com mit dem Service, Alternativen zum aktuell selektierten Buch anzubieten, die andere Kunden zusammen mit diesem Buch bereits bestellt haben. Als Grundlage setzt Amazon.Com für diesen Mechanismus die Transaktionsdaten der Bestellungen ein. Über Kunden-IDs und Transaktions-IDs läßt sich damit der Bezug zwischen verschiedenen Produkten herleiten. Wenn nun zufälligerweise das Buch „Elektronische Dienstmärkte“ [Merz99] von einigen Kunden bestellt wurde, die auch gleichzeitig „Die Firma“ von Grisham orderte, so macht dies wenig Sinn, wenn der aktuelle Kunde sich für das erste Buch interessiert. Folglich ist auch noch die Produktklassifikation der Bücher zu berücksichtigen: Hier läßt sich feststellen, daß die semantische Distanz zwischen Merz und Grisham zu groß ist, um „Die Firma“ zu empfehlen.

Schließlich muß eine Recommendation Engine berücksichtigen, daß sich Geschmäcker und Produkte im Laufe der Zeit ändern. Folglich ist auch das Transaktionsdatum zurückliegender Käufe ein wichtiger Einflußfaktor, um Empfehlungen mit der Aktualität zu gewichten.

6.4 Datenschutztechnologie für Kundenprofile

Die Verarbeitung von Kundenprofilen ist ein zweischneidiges Schwert: Zum einen hilft sie, durch Personalisierung und Automatisierung des Benutzerkomfort zu steigern. Das Profil dient hierbei als Informationsfilter für den individuellen Kunden, aber auch für den Anbieter, der z.B. automatisch Sonderangebote für „Ladenhüter“ generieren kann.

Die Kehrseite der Medaille liegt im Datenschutz, denn bereits heute ist der Bestand an Kundenadressen bei Handelsunternehmen ein wichtiges Kapital, das unter anderem auch über Adressenhändler extern kommerzialisierbar ist. Kundenprofile im Zeitalter von Online-Shops bieten neben Adressen noch ein Vielfaches mehr an Marketing-Information. Folglich ist es ein natürliches Bestreben der Anbieter, diese Informationen für eigene Zwecke oder als Produkt einzusetzen.

Im folgenden erfolgt eine Aufarbeitung und vergleichende Darstellung aktueller Standards für das Profilmanagement. Neben konzeptionellen und technologischen Aspekten werden auch Status und Perspektiven dieser Standards aus Markt- und Produktsicht dargestellt. Daß dabei die gegenläufigen Interessen „Datenschutz vs. Profiling“ nicht notwendigerweise im Widerspruch stehen müssen, soll im folgenden gezeigt werden. Dabei sollen zunächst einige aktuelle Profil- und Datenschutztechnologien untersucht werden. Anschließend lassen sich diese im Hinblick auf ihre Umsetzbarkeit in der Internet-Ökonomie bewerten.

6.4.1 Die Perspektive des Verbrauchers: Datenschutz vs. Data Mining

Bisher haben wir uns mit der händlerseitigen Perspektive gegenüber dem Profiling beschäftigt. Natürlicherweise ist es Anliegen des Händlers, aus diesen Rohdaten soviel Information wie möglich zu generieren, damit Marketing und Vertrieb möglichst in Echtzeit auf den tatsächlichen Bedarf zugeschnitten werden können. Die Standardisierung von Profil-Information bietet hier vielfältige Chancen, Zusatzgeschäfte durch Weitergabe der Profildaten zu generieren.

Aber diese Rechnung wird häufig ohne den Wirt und auch ohne den Gesetzgeber gemacht: Ist es überhaupt im Interesse des Benutzers, daß Daten weitergereicht werden? Welche Information besitzt der Kunde über die Art

und Weise, auf die seine Daten verarbeitet werden? In welchem Verhältnis steht die Weitergabe von Profildaten zur aktuellen Datenschutzgesetzgebung? Diesen Fragen könnte man durch restriktive gesetzliche Maßnahmen begegnen, die pauschal eine Verarbeitung von Profildaten untersagt. Dies würde jedoch die Händlerseite sehr schmerzhaft treffen und auch nicht jeder Kunde wird sich in jeder Geschäftsbeziehung durchleuchtet fühlen.

Schließlich ergibt sich dann die Frage, wie diese Anforderungen so auf der technischen Plattform des Internet erfüllt werden können, daß der erforderliche Mehraufwand einfach zu handhaben ist.

6.4.2 OPS

Siehe auch (<http://developer.netscape.com/ops/ops.html>)

6.4.2.1 Hintergrund

Der Open Profiling Standard legt Datenformate und Übertragungsverfahren fest, welche die Online-Registrierung vereinfachen und nebenbei das Problem des ungeschützten Transports der Informationen lösen sollen. Bis heute steht kein Standardformat zur Verfügung, das die wiederholte Eingabe identischer Informationen bei verschiedenen Diensteanbietern überflüssig macht und eine kontrollierte, geschützte Abgabe der Informationen ermöglicht.

Der Standard wurde von Netscape, Firefly (Spezialist für Management- und Benutzerprofile) und VeriSign, der führenden Zertifizierungsautorität, ins Leben gerufen. Neben einer Vielzahl weiterer Firmen, darunter IBM, Hewlett-Packard, Sun und Oracle, hat sich mittlerweile auch Microsoft dazu bereit erklärt, diesen Standard zukünftig in seinen Produkten zu unterstützen. Derzeit liegt er dem World Wide Web Consortium (W3C) im Rahmen des P3-Projektes zur Rezension vor.

Eine automatisierte Benutzeridentifizierung im Web ist bisher nur mit *Cookies* möglich. Sie sind jedoch nicht standardisiert und nur in relativ wenigen Internet-Werkzeugen implementiert; eine umfangreiche Nutzung findet nicht statt. Außerdem ist die Cookie-Technik von Diskussionen über mangelnde Sicherheit und fehlende Privatsphäre begleitet, daher ist eine nicht-verdeckte Handhabung von Benutzerdaten, die über HTML-Formulare eingegeben sind, empfehlenswerter. Zu den wesentlichen Nachteilen von Cookies zählen beispielsweise das Fehlen eines Zugriffsschutzes auf einzelne Attributwerte oder die ungeschützte Datenhaltung auf der Benutzerseite, die ein freies Manipulieren durch andere Benutzer zuläßt, insbesondere, wenn sich mehrere Benutzer einen PC teilen oder ein gemeinsames (Netzwerk-) Verzeichnis zur Ablage der Cookies verwendet wird..

Im Gegensatz zu Cookies soll OPS den Anwendern einen flexibleren Einsatz ihrer Benutzerprofile und eine wesentlich bessere Kontrolle der darin enthaltenen Informationen ermöglichen. OPS stützt sich neben dem Kommunikationsprotokoll HTTP auf zwei weitere Industriestandards: erstens auf vCard, einer Spezifikation des Internet Mail Consortium (IMC) zum Austausch von 'elektronischen Visitenkarten' unabhängig von der verwendeten Applikation oder vom Netz, zweitens auf digitale Zertifikate, also auf den Einsatz von Public-Key-Kryptographie zur Verifizierung der Identität. In diesem Zusammenhang wäre auch der Einsatz des X.509-basierten Zertifikatsmanagements denkbar.

Terminologie

- **Profil:** Ein hierarchische Ansammlung persönlicher Profilinformatoren mit Eigenschaften und Daten, die einen Endbenutzer beschreiben. Siehe auch das Beispiel weiter unten.
- **Profilattribut:** Ein elementares Datum, das eine Eigenschaft des Benutzers beschreibt.
- **Profil-Sektion:** Eine Gruppierung von Attributen und/oder untergeordneten Sektionen innerhalb eines Profils.
- **Top-level-Profil-Sektion:** Eine Sektion, die keiner übergeordneten angehört. Top-Level-Sektionen besitzen dedizierte *Top-level-Authorities*.
- **Permissions:** Das Recht, welches anderen gewährt wird, Profilattribute oder -sektionen entweder zu lesen oder zu schreiben.
- **Credentials:** Zusicherungen seitens Dritter im Hinblick auf die Identität, Berechtigung und Praxis eines Diensteanbieters.

- **Profile Request Object:** Ein Datenobjekt, welches an einen User Agent gesendet wird, um Profilattribute zu lesen. Es beinhaltet die Identität des Senders (Dienstanbieter) sowie Informationen über den Kontext, in dem dieses Objekt übertragen wird (z.B. Sitzungsnummer).
- **Profile Write Object:** Ein Datenobjekt, welches an einen User Agent gesendet wird, um Profilattribute zu schreiben.
- **Terms of Exchange:** Ein Text, der die beabsichtigte Verwendung der Profildaten beschreibt. Beispiel: "Der Anbieter des ADSL-Dienstemarktes wird die Profilinformaton nutzen, um eine bessere Personalisierung der ADSL-Portalseite zu erreichen."

6.4.3 Organisatorische Betrachtung

Folgende Parteien und Rollen sind im Szenario der Profilherausgabe und -nutzung beteiligt:

- **Endbenutzer:** Individuelle Benutzer, die ihre Profilinformaton verwalten.
- **User agents:** Software auf der Client-Seite, mit deren Hilfe Profile durch den Endbenutzer verwaltet, mit Dienstanbietern verhandelt und durch Leser oder Schreiber zugegriffen werden. Der User Agent abstrahiert von der Komplexität des konkreten Profils, um damit seine Verwaltung zu vereinfachen.
- **Dienstanbieter:** Profil-Leser oder -Schreiber, z.B., Web-Anbieter, die personalisierte Nachrichten, Börseninformaton zusammenstellen.
- **Profil-Leser:** Eine Partei (Dienstanbieter), die auf einen Teil des Profils zugreifen will und im Gegenzug einen Dienst anbietet.
- **Profil-Schreiber:** Eine Partei, die Profilinformaton hinzufügt oder modifiziert.
- **Section Authority:** Ein Profil-Leser, der spezielle Rechte zur Vergabe von Zugriffsberechtigungen für eine Sektion durch andere besitzt.
- **Access Providers:** Die Partei, die physikalischen Zugang zum Profil bietet. Dies kann der lokale Rechner des Benutzer sein oder auch ein Profilmanagement-System seitens eines Online-Dienstes.
- **Certificate authorities:** Vertrauenswürdige Dritte, die die Authentizität eines Benutzers (Profil-Leser oder -Schreiber) anhand von Zertifikaten zusichern.
- **Auditors:** Vertrauenswürdige Dritte, welche die Praktiken eines Profil-Lesers oder -schreibers verifizieren und dies durch entsprechende Zertifikate bescheinigen.

OPS-Nutzung in Verbindung mit HTTP

Profilübertragungen finden via HTTP im wesentlichen durch zwei Operationen statt: *Profile Write* und *Profile Read*. Ein Profile Write fügt den SetProfile-Header, ähnlich dem SetCookie-Header, dem HTTP-Datenstrom hinzu. Empfängt der Browser sowohl ein Profile Read (GetProfile-Header) als auch Profile Write, wird letzteres zuerst ausgeführt - eine einfache, aber wirkungsvolle Transaktionssicherung, da das anschließende Profile Read den zuvor beschriebenen Teil des Benutzerprofils verifizieren kann. Würde beim Schreiben von Profilinformaton nur der SetProfile-Header gesendet, wäre ungewiß, ob die Informaton auch tatsächlich beim Anwender gespeichert wurde.

Ein Profile Read ist im Gegensatz zum Profile Write ein zweistufiger Prozeß: Zunächst muß die Site, die dem Client einen GetProfile-Header sendet, genau wissen, welche Profilelemente sie erhalten möchte. Bevor die angefragten Daten übermittelt werden, verifiziert der Client den Request und wartet auf das O.K. seitens des Anwenders. Hat er der Übermittlung zugestimmt, prüft auch die Serverseite die Client-Angaben. Erst jetzt wird die gewünschte Informaton (etwa eine individuelle Internet-Zeitung) dem Benutzer in Form einer weiteren HTML-Seite zur Verfügung gestellt. Der gesamte Vorgang soll nach der derzeitigen Spezifikation unter Zuhilfenahme des SSL (Secure Socket Layer) erfolgen, das Kennwörter oder auch persönliche Informaton gesichert über das Netz transportiert.

Der angestrebte Standard wird sicherlich dazu beitragen, das Internet für kommerzielle Zwecke attraktiver zu gestalten. Anbieter können individualisierte Kundenbeziehungen über das Internet pflegen. Die Einbeziehung etablierter Internet-Standards wie HTTP, SSL oder auch digitale Zertifikate erlaubt die Nutzung vorhandener

Verfahren.

Derzeitige Mechanismen zur Benutzerauthentifizierung durch Cookies dürften durch das OPS-System ersetzt werden. Dennoch verschwinden Cookies vermutlich nicht vollständig - insbesondere bei Ad-hoc-Zugriffen, wie sie bei Online-Malls üblich sind. Hier stellen sie die Grundlage zur Zustandsverwaltung für virtuelle Einkaufswagen dar.

OPS-Beispielprofil

Der Open Profiling Standard definiert ein Profil als hierarchisierte Ansammlung von Attributen mit Name/Wert-Paaren, die in Sektionen und Subsektionen organisiert sind. Sogenannte Top-Level-Sektionen gehören keiner anderen an. Alle darin enthaltenen Informationen - bestimmt für eine definierte Domain - sind anderen Top-Level-Sektionen nicht zugänglich.

Eine Ausnahmeregelung kann der Benutzer jedoch explizit vorsehen. Die Profildaten sind durch einen MIME-Container repräsentiert, der dem MIME-Typ text/directory entspricht. Andere Kodierungsformate, die beispielsweise durch individuelle OPS-fähige Applikationen genutzt werden könnten, sollten allerdings mindestens OPS-kompatibel zum sogenannten vCard-Encoding sein. Das Diskussionspapier von Microsoft schlägt darüber hinaus unter anderem ein Interchange-Format auf Basis einer XML-Instanz vor. Demnach könnte ein Profil beispielsweise folgendes Aussehen haben:

```
<?XML version="1.0"?>
<PersonalData>
  <Contact>
    <UserID>Merz4711</UserID>
    <Email>merz@ponton.de</Email>
    <CommonName>Michael Merz</CommonName>
    <GivenName>Michael</GivenName>
    <FamilyName>Merz</FamilyName>
    <Address>
      <Line1>Internetweg 2</Line1>
      <City>Hamburg</City>
      <State>HH</State>
      <PostalCode>22391</PostalCode>
      <Country>Germany</Country>
    </Address>
  </Contact>
  <Demographic>
    <Birthday>19640318</Birthday>
    <Gender>M</Gender>
    <LevelOfEducation>14</LevelOfEducation>
  </Demographic>
  <Payment>
    <Method>Ecash</Method>
    <Currency>DM-DeutscheBank</Currency>
    <WalletVersion>0.8</WalletVersion >
  </Payment>
  <OrgData>
    <School>Einstein Gymnasium</School>
    <Grade>8</Grade>
  </OrgData>
</PersonalData>
```

6.4.4 P3P

P3P (*Platform for Privacy Preferences Project*) ist eine Standardisierungsbemühung, die dem einheitlichen Umgang mit Profilinformatoren dient. Sie wird vom Web-Consortium durchgeführt. Erste Standards der P3P-Gruppe werden voraussichtlich im Frühjahr verabschiedet werden. P3P wird in der Browser-Generation 5.x von Netscape und Microsoft eingesetzt werden. Dabei wird sich dieser Einsatz wahrscheinlich noch nicht auf alle Bereiche erstrecken, die vom P3P-Standard abgedeckt werden. Für Aufgaben des Datenaustausches (insb. für Profile und Protokolle für ihre Aushandlung) wird XML als Repräsentation der Protokolldateneinheiten verwendet.

Bis auf den XML-Standard befinden sich alle anderen Dokumente im Zustand "Draft" oder "Working Draft".

Die P3P-Familie setzt sich zusammen aus verschiedenen Teilstandards, auf die es aufsetzt, bzw. die zur vollständigen, einheitlichen Aushandlung von Profildaten und Verarbeitungspraktiken erforderlich sind:

- Einheitliches Vokabular für Profile und Datenschutzpraktiken ("Harmonized Vocabulary")
- P3P Syntax-Spezifikation
- Festlegung von Verhandlungsprotokollen
- APPEL (A P3P Preference Exchange Language)
- XML (Extended Markup Language)
- XML NameSpaces

Das Platform for Privacy Preferences Project des World-Wide-Web Consortium (W3C) dient als Plattform für vertrauensvolle und informierte Online-Interaktionen zwischen Dienst Anbietern und -nachfragern. Ziel von P3P ist es, WWW-Benutzer auf der Client- und Serverseite zu befähigen, Präferenzen hinsichtlich ihrer Datenschutzvorteilungen auszutauschen und Einigung zu erzielen. Teilnehmer werden damit in Kenntnis gesetzt, welche Datenschutzpraktiken auf der Serverseite zum Einsatz kommen.

Aufgabe dieser Technologie ist zum einen, Teilnehmern Gewißheit bez. der Weiterverarbeitung privater Daten zu geben, sie Einfluß auf diese Verfahren nehmen zu lassen und somit den gesetzlichen Regulierungsbestrebungen (zumindest im Raum der Europäischen Union) gerecht zu werden, ohne gleichzeitig die Verwertung von Profildaten vollständig zu unterbinden.

Schließlich wird das Web-Angebot dann nicht nur hinsichtlich inhaltlicher und ökonomischer Aspekte transparenter, sondern auch hinsichtlich der Verarbeitung persönlicher Daten. Ein Kopplung dieser Aspekte kann dabei durchaus auftreten, indem etwa ein Dienst seinen Kunden Rabatte einräumt, wenn sie ihm mehr Daten zur Verfügung stellen oder ihm erlauben, diese Daten auch an Dritte weiterzugeben.

6.4.4.1 Überblick

P3P wurde entwickelt, um *WWW-Benutzern* und *Dienst Anbietern* bei der Einigung auf das Profiling zu unterstützen. Dazu wurde ein Protokoll definiert, welches in seiner einfachsten Form aus einem *Angebot* (Proposal) und einer *Annahme* (Acceptance), die als HTTP-Nachricht eine *Einigung* (Agreement) beinhaltet. Im Rahmen der P3P-Aktivitäten werden z.Z. Variationen dieses Basisprotokolls entwickelt, um dem beteiligten Softwarekomponenten mehr Möglichkeiten zur Aushandlung von Profilen zu geben.

Haben sich Benutzer und Dienstanbieter auf ein Verfahren geeinigt, werden die betreffenden Informationen unter der betreffenden Agreement-ID gespeichert. Der Ort der Speicherung kann bei den beteiligten Parteien, aber auch bei einem vertrauenswürdigen Dritten liegen.

Ein Angebot bezieht sich auf einen *Bereich* (realm), für den die erklärten Praktiken gelten werden. Dieser Bereich ist üblicherweise die Web-Site des Anbieters und wird durch einen oder mehrere URIs identifiziert. Das Angebot besteht aus Erklärungen, welche Daten gesammelt werden, dem Zweck dieser Sammlung, mit wem die Daten ausgetauscht werden und ob die Daten auf eine bestimmte Weise genutzt werden. Zusätzlich kann das Angebot weitere Informationen enthalten wie

- einen *elektronischen Notar* (assuring party), der die korrekte Verarbeitung der Daten zertifiziert oder
- Informationen über das Verfügbarmachen bzw. Zurückhalten von Daten gegenüber dem Kunden (*disclosures*)

Um den Benutzer vom "manuellen" Aushandeln der Datenschutzpraktiken zu entlasten, werden Agenten (*user agents*) eingesetzt. Diese lassen sich über eine graphische Benutzerschnittstelle konfigurieren und treten für den Benutzer erst wieder in Erscheinung, wenn es Probleme beim Aushandeln der Praktiken gibt.

Anspruchsvolle P3P-Implementierungen werden *Repositories* unterstützen, in denen Benutzer für individuelle Anbieter entsprechende Konfigurationen ablegen können, d.h. welche Daten an welche Anbieter herausgegeben werden können. Im Repository liegt damit auch die vollständige Profilinformaton vor. Wenn eine Einigung erzielt wurde, können die betreffenden Informationen direkt aus dem Repository geladen werden. Gleiches gilt für Dienstanbieter: auch sie möchten u.U. Daten im Repository des Benutzers ablegen. Dabei entspricht das Repository der Funktion der Cookie-Datei, jedoch in für den Benutzer besser kontrollierbarer Weise. Diese Nutzung ist unabhängig von der herausgegebenen Profilinformaton: Ein anonymer Benutzer könnte beispielsweise keine persönlichen Daten herausgeben, jedoch dem Anbieter erlauben, persistente Sitzungsinformation abzulegen, um bei nachfolgenden Verbindungen eine individuelle Umgebung zu schaffen. Auch solche Präferenzen werden im Zuge des P3P-Protokolls zwischen beiden Parteien ausgehandelt.

Abstrakt betrachtet (d.h. auf der Kommunikationsebene), ist P3P ein Protokoll, das es erlaubt, anhand von HTTP

strukturierte Daten auszutauschen. Etwas anwendungsnäher (d.h. auf der Repräsentations- bzw. Darstellungsebene) wird XML eingesetzt zur Spezifikation der Syntax von Protokolldateneinheiten (mit Hilfe spezieller Datentypdefinitionen für P3P) sowie zur einheitlichen Kennung von Datenelementen in den Protokolldateneinheiten. Eine weitere Ebene höher (Anwendungsebene) finden wir die Festlegung der P3P-Semantik. Hierzu ist eine einheitliche Ontologie (Begriffsapparat) erforderlich, um die P3P-spezifischen Konzepte in interoperabler Form zu benennen. Als Rahmenwerk dient RDF für diesen Zweck. RDF legt ein einfaches Datenmodell fest, so daß es zur Beschreibung von Web-Ressourcen (HTML-Seiten, Web-Sites oder auch Literatur im allgemeinen) verwendet werden kann.

P3P wurde so entworfen, daß Anwendungen auf ganz unterschiedlichen Client-Geräten unterstützt werden können – einschließlich solcher, die nur über beschränkte Speicherkapazität verfügen oder nur schmalbandig kommunizieren können.

Nachfolgend ist ein Beispiel für den Vorschlag einer Datenschutzvereinbarung gegeben, die zunächst als natürlichsprachlicher Text und anschließend in P3P-Syntax formuliert ist. Dieser Vorschlag zählt die Datenelemente auf, die der Anbieter zu sammeln gedenkt und erklärt, wie diese verwendet werden. Er identifiziert außerdem den Anbieter und seinen Notar (XXX Begriff paßt nicht). Dieser attestiert, daß der Anbieter die nach außen dargestellten Verfahrensweisen auch tatsächlich umsetzt. Diese Zusicherung kann alternativ auch vom Anbieter selbst (oder einer anderen Teilorganisation) kommen, jedoch hat sich in der üblichen Geschäftspraxis die Zuschaltung eines unabhängigen Dritten als wünschenswert erwiesen. Bereits heute existieren Organisationen wie z.B. TRUSTe, die Web-Anbietern hinsichtlich ihrer Datenschutzpraktiken zertifizieren. Da z.Z. jedoch noch keine detaillierten gesetzlichen Rahmenbestimmungen existieren, kann es bei den jeweiligen Regelwerken der verschiedenen TTPs zu Abweichungen kommen. Hier ist erst Klarheit zu erwarten, wenn beispielsweise innerhalb der EU die Datenschutzdirektive in einheitlicher, rechtsverbindlicher Form umgesetzt ist. Natürlichsprachliche Version einer Datenschutzvereinbarung:

Natürlichsprachliche Vereinbarung

"Comics Online, registriertes Mitglied bei bei "DatenschutzNotar" (<http://www.DatenschutzNotar.de>"), gibt folgendes für ihr Web-Angebot unter den Seiten "<http://www.comics.com/Katalog>" bekannt:

Wir sammeln PageImpressions, Visits und AdClicks in unseren HTTP-Logdateien. Wir sammeln ebenfalls Ihren Vornamen, Ihr Alter und Geschlecht, um unser Web-Angebot speziell für Sie aufbereiten zu können. Außerdem verwenden wir diese Information für unsere interne Marktforschung und Produktentwicklung. Wir benutzen diese Daten nur in anonymer, nicht-personalisierter Form. Wir geben diese Daten nicht kommerziell oder aus anderen Gründen an Dritte weiter. Niemandem außerhalb unseres Unternehmens wird Einsichtnahme in die Profilinginformation geboten, auch Ihnen nicht. Es bestehen jedoch Möglichkeiten der Einspruchnahme, die Sie unserer Datenschutzzinformation unter <http://www.comics.com/PrivacyPractise.html> entnehmen können."

Daß ein solcher Text aus einer Liste von Stichworten automatisch generiert werden kann zeigt das Beispiel des P3P-Proposal-Generators im Anhang.

P3P-Version

```
<PROP realm="http://www.comics.com/ "
  entity="Katalog" agreeID="38f28d2d24a77"
  assurance="http://www.DatenschutzNotar.de">
  <USES>
    <STATEMENT purpose="1" recipient="0" id="0">
      <REF name="Web.Abstract.ClientClickStream"/>
    </STATEMENT>
  </USES>

  <USES>
    <STATEMENT purpose="2,3" recipient="0" id="0"
      consequence="Ein URL-Angebot, das Ihnen gefällt">
      <WITH>
        <PREFIX name="User.">
          <REF name="Name.First"/>
          <REF name="Bdate.Year" OPTIONAL="1"/>
          <REF name="Gender"/>
        </PREFIX>
      </WITH>
    </STATEMENT>
  </USES>
```

```

    </STATEMENT>
  </USES>

  <DISCLOSURE discURI="http://www.comics.com/PrivacyPractice.html"
    access="3" other="0,1"/>
</PROPOSAL>

```

Anhand dieses Beispiels kann man erkennen, welche Merkmale einen P3P-Vorschlag ausmachen:

- Zunächst werden Profilinformatoren standardisiert, damit jeder Server und jeder Browser in der Welt ihre Inhalte „verstehen“. Zu diesem Zweck ist im Beispiel das hierarchische Schema zu erkennen, das der Profilinformatoren zugrunde liegt. „Name“ setzt sich aus „First“ und „Last“ zusammen, Web-Server-Profile werden unterteilt nach „Abstract“ (anonyme Daten), die als Bestandteil wieder „ClickStream“ – also die Spur von „PageImpressions“ beim Server – enthalten können.
- Ferner wird über das Element USES deklariert, welche Informationen („WITH“) für welche Zwecke verwendet werden („purpose“). Hier läßt sich extrem feiner Ebene die Verarbeitung von Profilinformatoren beschreiben und aushandeln.
- Schließlich dienen Referenzen auf weitere Web-Seiten als Hinweis zum Datenschutzverfahren bzw. zu einer Trusted Third Party der weiteren Information des Benutzers. Die TTP wird als Vertrauenssichernde Maßnahme genannt, da davon ausgegangen wird, daß der Kunde dem Anbieter eher traut, wenn eine solche Instanz die Einhaltung Datenschutzrichtlinien überwacht.

Einigung erzielen

Die Idee des P3P-Agreement geht weit über eine "klassische" Vereinbarung per Fax oder schriftlicher Korrespondenz hinaus: Agreements binden vereinbarte Daten des Benutzers an Datenschutzpraktiken des Anbieters und ordnen diese wiederum individuellen URIs (Uniform Resource Identifiers) zu. Ein Agreement wird immer vom Anbieter vorgeschlagen und vom Teilnehmer abgelehnt, bestätigt oder in modifizierter Form als Gegenvorschlag zurückgeliefert. Es enthält Informationen zur Identifizierung des Anbieters und sollte alle relevanten Datenelemente zur Spezifikation der Verarbeitung privater Daten enthalten. Wenn ein Anbieter Daten des Teilnehmers sammelt, muß er dies über das Agreement mitteilen.

Proposals sind auf der Basis des Datenmodells des RDF-Standards kodiert. Die Syntaxdefinition von P3P spezifiziert eine RDF-Anwendung, die die Grammatik eines P3P-Proposal festlegt. Das "Harmonized Vocabulary" ist ein XML/RDF-Schema, welches spezifische Ausdrücke und Konstanten festlegt, die konform sind zur P3P-Grammatik.

Beispielsweise legt die P3P-Grammatik fest, daß der Zweck benannt ist, zu dem Daten gesammelt werden. Das Vokabular hingegen definiert die zulässigen Ausprägungen als Liste von sechs spezifischen Zwecken. Dennoch besteht die Möglichkeit, P3P für individuelles Vokabular einzusetzen, dann jedoch kann dieses natürlich nicht konform zum P3P-Standard sein und kann damit auch nicht von Standard-P3P-Software verarbeitet werden.

Für national unterschiedliche Gesetzgebungen und Regulierungen kann das Vokabular jedoch erweitert werden. Dabei kommen die Möglichkeit des XML-Namensraumes zur Geltung, mit deren Hilfe Dokumenttypdefinitionen (so auch die eines P3P-Statements) dynamisch erweitert werden können.

Kommunikation

P3P-Interaktionen beginnen üblicherweise, wenn ein Browser eine Web-Seite des Anbieters abrufen will. Als Antwort sendet der Server ein P3P-Proposal. Der User Agent des Browsers vergleicht nun das Proposal mit den Präferenzen des Teilnehmers. Bei Inkonsistenzen zwischen diesen Daten hängt es von der Konfiguration des User Agent ab: er kann diesen Sachverhalt durch ein Dialogfenster dem Benutzer melden, die Kommunikation abbrechen (durch das Senden eines "Reject") oder einen oder mehrere Gegenvorschläge machen. Auch weiterführende Erklärungen der Konsequenzen einer Sammlung von Benutzerdaten können vom Betreiber an den Benutzer gesendet werden, um den Hintergrund der Datensammlung näher zu erläutern.

Akzeptiert der Benutzer (oder sein Agent) das Proposal, sendet er einen elektronischen Fingerabdruck (d.h. einen Hash-Wert) an den Betreiber zurück. Diese Information heißt AgreementID. Steht genügend lokaler Speicher zur Verfügung, können Agreements dort abgelegt werden mit der AgreementID als Hash-Wert.

Nachdem Einigung erzielt wurde, sendet der User-Agent alle erforderlichen bzw. vereinbarten Daten an den

Server. Diese können entweder aus dem Repository des Benutzers oder über die Benutzerschnittstelle erlangt werden. Natürlich können auch Agreements erzielt werden, bei denen überhaupt keine Daten herausgegeben werden müssen.

Nachdem eine Sitzung beendet wurde, kann die bereits existierende AgreementID für spätere Sitzungen wiederverwendet werden. Dadurch wird bekannt, erstens daß bereits eine frühere Sitzung unter einem bestimmten Agreement stattgefunden hat, zweitens wird nochmals festgelegt, unter welchen Datenschutzvorgaben diese Sitzung durchgeführt wird und drittens werden dadurch automatisch jene Datenelemente nachgefragt, aufgrund dessen Agreements festgelegt wurden. Darauf kann der User-Agent mit einer direkten Antwort reagieren (Übergabe der Datenelemente) oder erneut den "vollen Wortlaut" des Agreements anfordern, wenn beispielsweise kein Repository zur Ablage von Agreements zur Verfügung stand.

Es sollte noch darauf hingewiesen werden, daß User Agents in unterschiedlicher Form zur Verfügung stehen können. Sie können als fester Bestandteil des Web-Browsers, als Plug-In, als Proxy-Server oder auf der Seite eines ISPs relaisiert sein. Sie können sich damit auf dem Rechner des Teilnehmers oder eines Servers befinden. Schließlich können sie mit oder ohne Repository implementiert sein. In jedem Fall agieren sie jedoch allein im Auftrage des Teilnehmers.

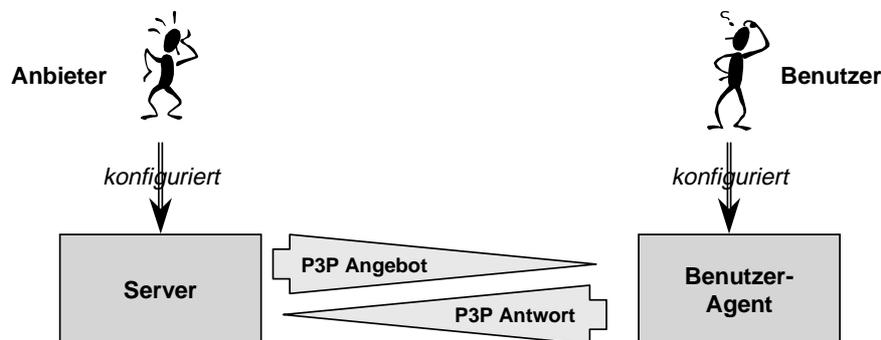


Abb. 22: Verhandlungsprotokoll von P3P

Datenkategorien

XXX Deutsch!

- *Physical Contact Information.* Information that allows an individual to be contacted or located in the physical world – such as phone number or address.
- *Online Contact Information.* Information that allows an individual to be contacted or located on the Internet - - such as email. Often, this information is independent of the specific computer used to access the network. (See Computer Information)
- *Unique Identifiers.* Non-financial identifiers issued for purposes of consistently identifying the individual -- such as SSN or Web site IDs.
- *Financial Account Identifiers.* Identifiers that tie an individual to a financial instrument, account, or payment system – such as a credit card or bank account number.
- *Computer Information.* Information about the computer system that the individual is using to access the network – such as the IP number, domain name, browser type or operating system.
- *Navigation and Click-stream Data.* Data passively generated by browsing the Web site – such as which pages are visited, and how long users stay on each page.
- *Transaction Data.* Data actively generated from or reflecting explicit interactions with a service provider through its site – such as queries to a search engine, logs of account activity, or purchases made on the Web.
- *Demographic and Socio-economic Data* Data about an individual's characteristics – such as gender, age, and income.
- *Preference Data.* Data about an individual's likes and dislikes – such as favorite color or musical tastes.

- *Content*. The words and expressions contained in the body of a communication – such as the text of email, bulletin board postings, or chat room communications.

P3P Statements und Requests

Es gibt 8 verschiedenen Typen für Statements und Requests, die über P3P abgewickelt werden können. Die Form dieser Dateneinheiten wurde erst kürzlich standardisiert:

1. *Request for data* – Ein Server fragt Daten vom User Agent ab.
2. *Request for practice*. Ein User Agent eröffnet eine Kommunikation, indem er Praktiken des Servers abfragt.
3. *Request for preferences* – Ein Server (Suchmaschine oder vertrauenswürdiger Proxy) fragt Präferenzinformationen des User Agent ab.
4. *Transfer of practice*. Mit dieser Dateneinheit überträgt der Server eine Erklärung, welche die Datenschutzpraktiken des Servers bez. spezieller Datenelemente des Benutzers erläutert. Im Rahmen des P3P-Vokabulars wird die Bedeutung dieser Statements standardisiert.
5. *Transfer of preferences*. Als Antwort auf die vorherige Erklärung, kann der User Agent seine Präferenzen an einen vertrauenswürdigen Mittler übertragen.
6. *Request for transfer of data*. Hiermit fragt der Server konkrete Daten beim User Agent ab. Diese Nachricht kann mit dem „Transfer-of-Practice“-Statement kombiniert sein.
7. *Agreement*. Diese Nachricht sendet der User Agent an den Server, wenn er mit dessen Erklärung einverstanden ist, d.h., wenn es zu keinem Konflikt beim Matching der beiden Policies kam. Anderenfalls kann die Antwort auch eine vorläufige oder endgültige Ablehnung, je nachdem, ob der User Agent eine Verhandlung zulässt oder nicht.
8. *Transfer der Daten*. Dies kann in Verbindung mit dem „Agreement“-Statement erfolgen.

Statements 1, 4 und 6 können auch gemeinsam vom Server gesendet werden. Der *Request for Data* und der *Request for Transfer of Data* wurden als getrennte Nachrichten implementiert, um unterschiedliche Verhandlungsmechanismen zuzulassen, die in zukünftigen P3P-Protokollen implementiert werden könnten.

6.4.5 Bewertung: OPS und P3P im Vergleich

OPS wurde von Netscape in Verbindung mit Firefly Network und VeriSign entwickelt. Es erlaubt Benutzern, persönliche Daten auf dem PC zu speichern und über ihre Herausgabe nach Web-Anbietern individuell zu entscheiden. Das Profil kann sich aus Namen, Adresse, Geschlecht, Familienstand, Telefonnummer, E-Mail-Adresse, persönlichen Hobbies, Produktkategorien etc. zusammensetzen.

Datenschutz- und Verbraucherschutzorganisationen geht diese Maßnahme jedoch noch nicht weit genug, da sie nur die Anwenderseite adressiert: über Verarbeitungspraktiken des Anbieters wird bei der Festlegung der freizugebenden Daten nichts ausgesagt. Gerade diese Information ist jedoch für den Kunden relevant, wenn er Verfahrensregeln definieren will, die zu den unterschiedlichen Verarbeitungspraktiken die "passende" Freigabepolitik festlegt.

Als Folge dieser Inflexibilität wurde die Gefahr gesehen, daß Kunden aus Bequemlichkeit eher mehr als weniger Information preisgeben, um Konflikte mit angebotenen und nachgefragten Profilen zu vermeiden. Dies erlaubt Web-Anbietern, die Freigabe von Profilinformatoren – z.B. zur Registrierung – abzufordern. Benutzer können sich zwar weigern, jedoch müssen sie dann in Kauf nehmen, sämtliche Daten selbst einzugeben.

Der OPS-Standard wird bereits von mehr als 100 Technologie-Unternehmen unterstützt. Die Verwendung von OPS entspricht damit der US-Politik, Datenschutzfragen der Industrie in Form freiwilliger Selbstregulierung zu überlassen.

In ähnlicher Weise arbeitet P3P, nur daß Anbieter hier ihre Praktiken offenlegen müssen. Dabei wird das Vokabular zur Festlegung von Verarbeitungs- und Weiterleitungsmöglichkeiten einheitlich festgelegt. Jedoch besteht damit noch keine Handhabe, die erklärten Praktiken auch tatsächlich umzusetzen. Beide Verfahren beruhen heute noch auf einer freiwilligen Selbstkontrolle auf der Anbieterseite.

P3P strebt an, durch Verbraucherschutzorganisationen Schablonen entwickeln zu lassen, die als Konfiguration vom Benutzer übernommen werden können.

6.5 Virtuelle Shops & Malls

Wenn Endkunden nennen sollten, welche Arten von Anwendungen sie sich unter "Electronic Commerce" vorstellen können, steht sicherlich das Stichwort "Online Shops" ganz oben auf der Liste. Das Shop-System ist schließlich die Schnittstelle zwischen Kunde und Händler beim B2C-Commerce. Online Shops existieren bereits seit einigen Jahren, so daß insbesondere in diesem Bereich etliche Erfahrungen gesammelt werden konnten. Intershop als einer der prominentesten Vertreter wurde bereits 1994 zum ersten Mal ans Netz gebracht. Inzwischen liegt das Geschäft mit den Shops jedoch nicht mehr allein in der Hand spezialisierter Anbieter wie Intershop, Netscape oder iCat – auch IBM, Oracle, Microsoft etc. haben eine Shop-Lösung ihren Anwendungsarchitekturen hinzugefügt.

Ein Online-Shop ist jedoch ein weitaus komplexeres Konstrukt als die Webseiten, die sich dem Benutzer darstellen. Bei jeder Navigation durch den Shop ist eine große Anzahl Datenbankzugriffe erforderlich, serverseitige Skripts werden ausgeführt und häufig sind Anwendungsprozesse beteiligt, die beim Anbieter auf eine große Anzahl an Rechnern verteilt sind.

Bevor wir uns nun jedoch solche Systeme genauer anschauen wollen, sollte zunächst geklärt werden, welche Aufgabe ein Shop-System erfüllen sollte:

Was wird verkauft?

Heute online erhältliche Produkte schließen Hard- und Soft-Goods ein. Im Falle von Hard-Goods ist eine enge Integration des Shop-Systems in die Warenwirtschaft des Unternehmens erforderlich, da physische Prozesse wie die Auslieferung, Nachbestellung oder Produktionsaufträge an andere Abteilungen oder externe Partner veranlaßt werden müssen. Aus diesem Grunde beinhalten Systeme wie beispielsweise Intershop gleich eine vollständige Warenwirtschaft, mit der Lagerbestände und damit verbundene Prozesse verwaltet werden können.

Eine völlig andere Kategorie sind Soft-Goods, also Produkte, die sofort online ausgeliefert werden können. Als Beispiele sind hier die Software-Distribution, Audio-Clips, Schriften oder Dokumente zu nennen. Hier ist natürlich keine Anbindung an irgendeine Lagerbestandsverwaltung erforderlich. Statt dessen ergeben sich andere Klippen, die es zu umschiffen gilt: Es muß beispielsweise sofort die Bezahlung veranlaßt werden, während bei Hard-Goods die Zahlungsautorisierung verzögert erfolgen kann. Ergibt diese Prüfung, daß der Kunde nicht liquide ist, kann der Vorgang noch vor Auslieferung des Produktes abgebrochen werden. Wenn eine Zahlungsautorisierung erfolgreich war, kann die eigentliche Abbuchung mit zeitlicher Verzögerung stattfinden. Stellt sich innerhalb dieser Zeit heraus, daß die Liquidität des Kunden erschöpft ist, trägt das Kreditkartenunternehmen das Risiko. Aber nicht nur die sofortige Bezahlung von Soft-Goods wirft Probleme auf, auch der Zugriff auf die gekauften Produkte: wie soll der Kunde diese laden? Man würde vielleicht vorschlagen, daß der Kunde seine e-Mail-Adresse im Web-Formular einträgt und nach erfolgreicher Bezahlung das Soft-Good erhält. Hier sind allerdings folgende Punkte zu beachten:

- Erstens ist die per Hand eingetragene e-Mail-Adresse in 5-10% aller Fälle fehlerhaft. D.h. ein Mitarbeiter muß nun nach der richtigen Adresse recherchieren, was unnötigen Zeitaufwand kostet. Ist die Gewinnspanne bei diesem Produkt niedrig, kann ein solcher Eingriff in 10% aller Fälle bereits spürbare Auswirkungen auf die gesamte Rentabilität des Online-Geschäftes haben. Gehen wir einmal davon aus, daß die Korrektur einer E-Mail im Durchschnitt 15 Minuten dauert und daß dieser Aufwand 25 DM kostet, dann ist sind wir bei einer Gewinnspanne von 10 DM pro Artikel bereits mit einer Reduktion von 25% konfrontiert.
- Zum zweiten müssen wir trotz aller Stabilität des heutigen Netzes und der Hardware mit Unterbrechungen und Ausfällen rechnen. Daher ist die Bereitstellung einer befristeten Download-Möglichkeit für das Soft-Good eine weitere Voraussetzung für den Online-Handel. Wenn hier nämlich wieder eine E-Mail nicht weitergeleitet werden kann, wird sich der Kunde beschweren, und es ist wieder ein zeitaufwändiger Prozeß nachzuprüfen, ob er als Kunde registriert ist und das Produkt bezahlt hat. Aus diesem Grunde werden üblicherweise flexible Mechanismen zur Steuerung des Download eingesetzt. Zu beachten ist hierbei, daß die kundenindividuelle Konfiguration von Artikeln unter Verwendung der Kundenkennung angezeigt wird, so daß ihm eine Liste von URLs für den Zugriff auf die Produkt-Dateien generiert werden kann. Einige Produkte (z.B. der PublishingXpert von Netscape) unterstützen hier sehr differenzierte Modelle zur Abrechnung von Zugriffen.
- Soft Goods können schließlich auch kontinuierlicher Art sein, also Video- oder Audio-Clips. Allerdings hat sich die Diskussion um Themen wie etwa Video-On-Demand heute wieder erheblich abgekühlt. Dennoch ist eine Verschiebung weg vom "Business Modell" der Online-Videothek hin zu Streaming-Anwendungen mit kommerziellem Inhalt – z.B. beim Business-TV – festzustellen. Moderne Verfahren wie etwa Real Video (<http://www.real.com>) erlauben die zeitbasierte Abrechnung der Server-Nutzung. Dabei ist ebenfalls ein Be-

zahlungsmodell zu wählen, welches einerseits die tatsächliche Online-Nutzung exakt bemißt, andererseits allerdings dem Kunden nicht das schlechte Gefühl gibt, permanent sein Portemonnaie zu erleichtern. Psychologisch erscheint es einfacher, einem Kunden einen monatlichen Festbetrag von – sagen wir – DM 50,-- aufzuoktroieren, auch wenn er nach seiner üblichen Gewohnheit nur DM 30,-- verbrauchen würde. Er kann sich aber hingegen sicher sein, sein Kostenlimit nicht zu übersteigen. Auch für den Dienstanbieter ist dieses Modell meistens einfacher, da die Abrechnung lediglich auf Subskriptionsbasis erfolgt. Spontane Kunden, die befürchten, am Ende bei unzähligen Shops Abonnent zu sein, schreckt dies allerdings ab, da sie nun auf einer übergreifenden Ebene die Kostenkontrolle verlieren können. Insbesondere für die hier erforderliche "Spontan-Abrechnung" sind Micropayment-Verfahren entwickelt worden (Siehe Abschnitt XXX), die sich jedoch bis heute noch nicht durchsetzen konnten.

Wie wird verkauft?

Nachdem wir nun die Art der Produkte näher betrachtet haben, stellt sich die Frage, auf welche Weise der Verkaufsprozeß organisiert wird. Dazu ein Szenario:

Es ist 3 Uhr nachts und ein Kunde möchte mit einigen Gedichten die noch etwas magere Hochzeitszeitung anreichern, die er bis zum nächsten Tag fertigstellen muß. Er wendet sich an "Poem Online" und ist zunächst mit der obligatorisch Bitmap-lastigen Home-Page konfrontiert. Im nächsten Schritt wendet er sich an den Produktkatalog, der über verschiedene Selektionskriterien verfügt. Mögliche Einstiegspunkte in den Katalog sind u.a.:

- Der Name des Dichters
- Die Sprache des Gedichts
- Die literarische Periode
- Die Länge des Gedichts
- Sein Preis

Im Katalog sind 10.000 Gedichte erfaßt, so daß eine flexible Navigationsunterstützung zwingend erforderlich ist. Eine Klassifikation nach nur einem Kriterium (Periode oder Dichter) führt zu endlosen Listen von Einträgen oder Unterverzeichnissen. Ideal ist eine flexible Kombinierbarkeit der Suchkriterien, so wie es beispielsweise für den FontExplorer@Web von Linotype entwickelt wurde (Siehe Abschnitt XXX). Standardprodukte für Shopsysteme bieten in der Regel nur eine einfach strukturierte Kataloghierarchie, welche die Erwartung des Kunden hinsichtlich der Navigation nur unzureichend durch geeignete Produktkategorien befriedigen kann.

Sobald der Kunde zu einer Produktseite im Katalog gelangt ist, werden ihm Meta-Informationen sowie das Produkt selbst angeboten. Die Meta-Informationen entsprechen den oben genannten Kriterien, nach denen das Produkt klassifiziert worden ist. Auch weitere Schlüsselwörter für die Volltextrecherche zählen dazu. Als unmittelbare Produktinformation – also nicht auf der Metaebene – dient im Falle der Gedichte das Produkt selbst. Bei Soft-Goods wie Audio-Clips, Fonts oder online bestellbaren Büchern könnte ohne Probleme als "Teaser" (Appetithäppchen) ein Auszug geboten werden: dies könnte ein kurzer Ausschnitt des Clips, eine Bitmap des Fonts oder das Inhaltsverzeichnis des Buches sein. Weitere Informationen wie Kommentare anderer Käufer, Empfehlungen, Kontaktmöglichkeiten zum Autor/Künstler oder Editor runden die Möglichkeiten zur Produktinformation ab. Speziell beim Gedicht, das im Extremfall gar nicht auszugsweise dargestellt werden kann, bleibt dem Shop-Betreiber häufig nur die Möglichkeit, per Banner-Werbung seinen Umsatz zu realisieren.

Nach der Produktinformation tritt beim nächsten Schritt der *elektronische Einkaufskorb* (Shopping Basket, Shopping Cart) in den Vordergrund. Zum Einkaufskorb gelangt man, indem auf der Produktseite der entsprechende "add to shopping basket"-Button angeklickt wird. Im Einkaufskorb sammeln sich alle auf diese Weise eingetragenen Artikel, deren Anzahl hier meistens noch bestimmt werden kann. Ein Einkaufskorb ist dabei ein zustandsbehafteter „Überbau“ auf dem zustandslosen HTTP-Protokoll. Also müssen Mechanismen wie Cookies verwendet werden, um beim nächsten "add to shopping basket" festzustellen, daß bereits andere Produkte hineingelegt wurden. Wenn nun der Benutzer die Verwendung von Cookies verweigert, bleiben dem Shop-Betreiber weitere Möglichkeiten, den Zustand des Korbs zu bewahren. Üblich ist die Vergabe einer Session-ID bei jedem Eintritt in den Shop. Diese Session-ID wird in die HTML-Seite (egal ob im Katalog, als Produkt-Seite oder woanders) so hineingeneriert, daß bei Klicken auf einen Link oder einen Button, diese wieder an den Shop-Server zurückübertragen wird. Jede relevante Information kann nun in der Shop-Datenbank gespeichert werden.

Idealerweise sollte ein Shoppingbasket für eine gewisse Zeit persistent sein, damit ein Kunde, der während des Stöberns im Katalog ausschweifende Reisen zu anderen Servern durchführt, am Ende wieder den letzten Zustand vorfindet. Diese Funktion bieten einige Shop-Systeme, bei denen eine entsprechende Verfallsfrist in Tagen fest-

gelegt werden kann. Ist die Kunden-ID dem Shop-System bekannt, kann der Einkaufskorb auch nach einem Wechsel zu einem anderen Client-Rechner weiter gefüllt werden. Dazu ist jedoch eine Registrierung als Kunde erforderlich:

Wenn wir es nicht mit anonymen Payment-Verfahren zu tun haben (und das ist heute fast ausschließlich der Fall), ist meistens beim Kauf die Nennung von Kundendaten erforderlich. Diese umfassen mindestens die Informationen, die für die Kreditkartenzahlung erforderlich sind (Name, Kartenummer, Ablaufdatum, evtl. Card Holder). Darüber hinaus möchte der Shop-Betreiber natürlich weiteres über seine Klientel wissen: Adresse, e-Mail, Position, Einkaufsbudget ;-) etc. Jedes Shopsystem verfügt hier über eine entsprechende Kundendatenbank, deren Schema meistens so erweitert werden kann, daß jeder Wunsch des Betreibers erfüllt wird. Allerdings ist auch hier abzuwägen, daß ein Kunde den Einkauf verweigert, wenn er zu viele Daten über sich herausgeben muß.

Nachdem der Kunde bei unserem Poem-Online-Shop eingetragen wurde, ist schließlich der "Point-of-no-Return" erreicht: er muß bezahlen. Hier hängt es vom konkreten Anwendungsfall ab, welche Daten er auf seinem Order-Formular findet: das mindeste ist der Gesamtpreis aller Artikel, die auf der Liste stehen. Bei Hard-Goods sind üblicherweise noch Lieferkosten zuzuschlagen. Bei allen Gütern ist des Weiteren die Mehrwertsteuer zu berechnen. Bei Großkunden könnten schließlich noch diverse Kunden- oder Artikelrabatte zu berücksichtigen sein. Außerdem sind bei fast jedem Shop-System noch Promotion-Artikel definierbar, die mit einem Sonderpreis behaftet sind. Ist dies der Fall, überlagert er natürlich den Listenpreis und evtl. alle anwendbaren Rabatte. Hier kann die Produkt- und Rabattdefinition des Shop-Betreibers schnell unübersichtlich werden – eben genauso wie beim physischen Händler. Die Datenmodelle der Shopsysteme sind daher gerade in diesem Bereich sehr komplex. Um jede erdenkliche Eventualität abbilden zu können, sind sie daher in der Regel noch zu erweitern. Während alle bisherigen HTML-Seiten in der Regel ungesichert übertragen wurden, sollten die Order-Seiten jedoch über eine SSL-Verbindung geladen werden. Dies gilt insbesondere für die Kommunikation, bei der Kunden- und Kreditkarteninformationen übertragen wurden.

Nachdem der Kunde nun mit allen Details seines "elektronischen Angebots" zufrieden ist, klickt er den "Point-of-no-Return"-Button und hofft, daß nach den 20-30 Sekunden Wartezeit alles gut geht. Es läuft jetzt in der Tat ein komplexer Clearing-Prozeß im Hintergrund ab: abhängig vom Zahlungsverfahren (siehe Kapitel XXX) werden die Orderdaten an das Shopsystem übertragen. Dieses aktiviert zuerst eine händlerseitige Software-Komponente, die ihrerseits anschließend eine Verbindung zum Payment-Gateway aufbaut. In der Regel werden Händler-Software und Gateway-Software als Produkte von Anbietern zugekauft, die sich auf das Clearing von Zahlungen spezialisiert haben. In vielen Fällen ist das Payment-Gateway (wie der Name schon sagt) nur eine Vorstufe zum Server der Kreditkartengesellschaft, der erst in der Lage ist, Buchungen durchzuführen. Nun ist auch klar, warum dieser Prozeß 30 Sekunden dauern kann: Vom Kunden über den Shop und das Gateway zum Clearing-Server und zurück sind oft sechs "Hops" erforderlich, zzgl. diverser weiterer in den Intranets der beteiligten Parteien sowie diverser Datenbankzugriffe. 30 Sekunden wirken da schon fast schnell...

Da Online-Shops beim B2C-Commerce von Endkunden genutzt werden, ist die Benutzerfreundlichkeit von besonderer Bedeutung – insbesondere bei wachsender Online-Konkurrenz, die ja nur einen Mausklick entfernt liegt. Auch hier sind etliche Zielkonflikte zu lösen: Die schlichteste Methode (SSL plus HTML-Maske zur Eingabe der Kreditkartennummer) ist bei Ad-hoc-Käufen häufig auch die angenehmste. Alle weiteren Methoden, welche eine Wallet-Software erfordern, setzen die Zugangsschwelle für Benutzer ohne Wallet herauf. Nur wenn ein einziger Wallet-Standard sich als Plug-In aller gängigen Web-Browser etabliert hat, ist zu erwarten, daß die Vorteile seiner Benutzung quasi "aufgezwungen" werden können. Die heute gängige Wallet-Software hat im wesentlichen zwei Probleme: Entweder ist ein prohibitiver Installationsprozeß erforderlich (z.B. bei CyberCash und SET), der Endkunden eher veranlaßt, zur SSL-basierten Konkurrenz zu gehen oder die Wallet-Software wird unmittelbar für den individuellen Kauf vom Shop-Server als Java-Applet geladen (Brokat's X-Pay). In beiden Fällen spricht eine bessere Verschlüsselung und das "Vorbeischleusen" der Zahlungsinformation am Händler für den Einsatz dieser Systeme, die "Usability" leidet jedoch. Und im Eifer des Kaufes (man denke an die späte Hochzeitszeitung – inzwischen ist es bereits halb vier!) zählt der rasche Einkaufsvorgang für den Konsumenten häufig mehr als perfektionierte Sicherheit.

Nach dem "Point-of-no-Return" erhält der Kunde eine Auftragsbestätigung, auf der relevante Transaktionsdaten erfaßt sind. Dieses HTML-Dokument kann man sich ausdrucken oder auf sonstige Weise in die Finanzbuchhaltung übernehmen (dies ist natürlich ein Medienbruch!). Alternativ können diese Daten auch per E-Mail zugesendet werden; hier kann es jedoch aufgrund von Falscheingaben schnell zu Übermittlungsfehlern kommen. Bei Soft-Goods ist neben der Auftragsbestätigung noch ein Zugang zum Download erforderlich. Natürlich können die betreffenden URLs nicht direkt auf die Produkt-Datei verweisen – dann würde der Kunde die URL an alle Freunde verteilen. Es ist vielmehr sicherzustellen, daß nur er auf "seine" Produkte zugreifen kann und dies evtl. nur für eine begrenzte Zeit. Anbieter von Shop-Systemen unterstützen dies durch verschlüsselte URLs, die beispielsweise auf kundenspezifische Datenbankeinträge verweisen oder ein Server-Skript mit der entsprechenden Information parametrisieren.

Beim Linotype Font-Shop ist es beispielsweise möglich, noch nach Jahren einmal erworbene Produkte nachzuladen. Linotype gewährt ein lebenslanges Zugriffsrecht. Mit jedem weiteren Kauf verlängert sich also die Liste der Produkte, die für einen Kunden ad hoc zu konfigurieren ist.

Im Falle von Hard-Goods kann eine Integration mit dem Trackingsystem für Produktion und Auslieferung erfolgen: Hier wird dem Kunden ein individueller Zugang bereitgestellt, der beispielsweise auf die Produktionsdatenbank zugreift ("Ihrem Wagen wird gerade der Motor eingesetzt") oder der mit der Logistiksteuerung des Speditors kurzgeschaltet ist ("Die Kiste Bananen steht am Kai 17 und wartet auf die Zollabfertigung").

Shopping Malls

Was man bei Buchhaltungssystemen "Mandantenfähigkeit" nennt, findet sein Gegenstück bei Shop-Software im Mall-System. Aus der Benutzerperspektive bietet ein Mall-System im wesentlichen eine einheitliche Gestaltung der Benutzerschnittstelle (man weiß aufgrund des Layouts, daß sich die Weinhandlung, in der man sich befindet zum T-Shop gehört und nicht zum Shop.de). Zudem sind die Einzelshops integriert durch einen Metakatalog bzw. Anbieterverzeichnis sowie die Möglichkeit, per Suchfunktion Artikel aller Shops zu finden. Weitere Merkmale sind eher "haptischer" Natur: Wurde die Mall-Methapher wörtlich übernommen, so daß man sie virtuell durchwandern kann, oder wurde von einer räumlichen Ordnung vollständig abstrahiert? Wurde der Mall ein bestimmtes Motto zugrundegelegt (Ecomall, <http://www.umwelt.de/ecomall>)? Ferner finden Malls durch sprachliche oder geographische Regionen (z.B.: Electronic Mall Bodensee, <http://www.emb.net>), Branchen (Auto, Immobilien, ...) ihr individuelles Alleinstellungsmerkmal.

Es sind dabei mindestens noch die Perspektiven der Shop- und der Mall-Betreiber zu berücksichtigen: Der Shop-Betreiber möchte evtl. die Entwicklungs- und Abrechnungskosten weitestgehend auslagern, weil ihm im Hause die Kapazität nicht zur Verfügung steht. So bietet ein Autor im Selbstverlag vielleicht nur 5 Bücher an, die inklusive Metainformation auf einer HTML-Seite angeboten werden können. Eine Mall bietet hier die Möglichkeit der professionell betriebenen Abrechnung von Verkäufen sowie der "nahtlosen" Integration der Shop-Seite des Autors. Im Falle von Hard-Goods geht der Trend sogar zur Verwaltung des Auslieferungslagers und der Zustellung durch den Mall-Betreiber, wenn dieser mit dem Logistiksystem der anderen Dienste integriert ist. Hier ist Federal Express zu nennen mit ihrem Angebot zur integrierten Bestellabwicklung. Der Shop-Betreiber hat dem Mall-Anbieter eine Lizenzgebühr für die Shop-Nutzung sowie üblicherweise eine zeit- und umsatzabhängige Provision zu entrichten.

(FedEx XXX Beispiele).

Für den Mall-Betreiber liegt das kommerzielle Interesse in der Steigerung der Anzahl und Qualität der Shops und damit in der Steigerung der Besuche und Transaktionen. Nur durch Nachweis dieser Zahlen kann dieser im weiteren auch Werbekunden gewinnen, die – neben den Lizenzentnahmen der Shop-Betreiber – zur Umsatzsteigerung führen. Ein essentieller Mehrwert des Mall-Betreibers ist sicherlich die Abwicklung der Bezahlung. Hier kann der gesamte betriebswirtschaftliche Prozeß des Inkasso zentralisiert werden. Über die reine Zahlungsabwicklung hinaus bieten Mall-Anbieter auch Zusatzdienste, wie Bonitätsprüfungen von Kunden oder Werbeaktionen. Der einzelne Shop-Betreiber erhält lediglich eine monatlich konsolidierte Abrechnung. Auch der gestalterische Prozeß kann seitens des Mall-Betreibers zentralisiert werden. Ist der Shop-Betreiber nicht mit der Erstellung ansprechender HTML-Seiten vertraut, kann dies einige 10.000 DM kosten.

Weitere Funktionen eines Online-Shops

Das Shop-System als Kern macht heute nicht mehr das Hauptgeschäft der Anbieter von Shop-Software aus. Vielmehr sind es die Add-Ons und Plug-Ins, die vom Anbieter, dem Shop-Betreiber oder Dritten entwickelt werden. Auf diese Weise werden ursprünglich für Hard-Goods entworfene Systeme wie z.B. Intershop auch für Soft-Goods tauglich (XXX z.B. durch Erweiterungen wie ESD – Electronic Software Download). Angeboten werden daher u.a. folgende Erweiterungen:

- *Statistik- und Data-Mining-Systeme.* Die Datenbasis, die sich mit der Zeit aus Transaktionsinformationen, vor allem aber auch aus aufgezeichneten Besuchspfaden durch die URLs des Shops ergeben, sind für den Betreiber eine Goldgrube: er kann jetzt nicht nur individuelle Kundenvorlieben kennenlernen und auf automatisierte Weise darauf reagieren, sondern auch Zusammenhänge unabhängiger Käufe beliebiger Kunden erkennen. Auf diese Weise lassen sich Trends schneller erkennen und auch aktuell nachgefragte Produktkombinationen schneller identifizieren. Die Datenbasis des Shopbetreibers stellt somit selbst ein neuartiges Anlagegut dar, welches in dieser Präzision bisher noch nicht zur Verfügung stehen konnte. Natürlich sind Informationen dieser Datenbank (auch anonymisiert) veräußerbar, so daß hier für den Shop-Betreiber zusätzlicher Umsatz generiert werden kann. In der Zukunft sind aufgrund der Weiterentwicklung von Data-Warehouse-

Anwendungen sowie der Standardisierung (und damit Interoperabilität) der Transaktionsdaten sicherlich noch interessante Produktentwicklungen und Geschäftsmodelle zu erwarten.

- *EDI-Integration.* Da im B2B-Bereich EDI oder ähnliche Austauschformate eingesetzt werden, ist eine Integration mit dem Shopsystem besonders dann hilfreich, wenn Shop-Prozesse wie etwa das Bezahlen, die Bestellung und die Auslieferung zwischen Shop-Betreiber und Dritten auf dieser Basis betrieben werden. Neben dieser "klassischen" Nutzung von EDI zwischen Händler und Dritten bieten neuere Ansätze zudem die Möglichkeit, durch Plug-Ins oder nur HTML, EDI-Nachrichten als Dateneinheiten zwischen dem Web-Browser des Kunden und dem Händler zu versenden. Der Vorteil besteht hier in der unmittelbaren Überführung der eingegebenen Transaktionsdaten des Kunden in die Anwendungssoftware des Händlers.
- *Tax-Systeme.* Die Anwendung des korrekten Steuersatzes sowie der Abwicklung von Steuerbemessungen und -zahlungen im internationalen Handel rechtfertigt häufig dedizierte Plug-Ins, die als Gateway zur Finanzbuchhaltung des Shop-Betreibers, aber auch des Kunden verstanden werden können. (XXX Recherchieren: Oracle's Taxation Cartridge).
- Payment-Gateway
- Customer-Relation-Management
- Search-Engine
- Integration in die FiBu
- Integration in die WaWi
- XXX

6.5.1 Shop-Architekturen und Varianten

Die meisten Shop-Systeme besitzen folgende grundlegende Softwarekomponenten:

- *Shop-Datenbank mit Produktinformation.* Um Produktinformationen, die zig-tausendfach vorliegen können, überhaupt effizient verwaltbar und zugreifbar zu machen, ist eine Produktdatenbank im Back-End unumgänglich. Dabei ist festzulegen, wie Produktinformationen kategorisiert werden, welche Attribute den Produkten zuzuordnen sind, welche Ausprägungen diese Attribute haben können etc. Aber auch flankierende Informationen wie Rabatte, Links auf ähnliche Produkte, Bilder, Beschreibungstexte und Werbeeinstreuungen sind so in der Datenbank zu organisieren, daß erstens eine Aktualisierung der Produktinformation und zweitens ein einheitliches Auslesen ermöglicht werden kann. Zudem hat jeder Shop-Betreiber individuelle Erweiterungswünsche hinsichtlich der Datenbank und ihres Inhalts, so daß bereits eine erschöpfende Definition der Produktdatenbank ein kleines Beratungsprojekt darstellt. Weitere, typische Features der Produktdatenbank sind Staging-Areas (zur internen Simulation eines aktualisierten Shop-Systems bevor es "Life" geschaltet wird).
- *Administrationsdatenbank.* Neben dem Inhalt der Produktdatenbank fallen diverse weitere Verwaltungsinformationen an: Dies beginnt mit der Festlegung des Einstiegspunkts in den Shop, z.B. als URLs für CGI-Skripte, der Festlegung von Parametern für das Payment-Gateway, der Datenbankschemata für Kunden-, Lagerbestands-, und Transaktionsinformation. Die Administrationsdatenbank läßt sich, genauso wie die Produktdatenbank, über ein Web-Interface administrieren. Auch hier ist es allgemein üblich, diese Funktionen über unterschiedliche TCP/IP-Portadressen zugänglich zu machen. Dies bietet dem Firewall-Administrator die Möglichkeit, Autorisierungs- und Authentisierungsmechanismen flexibel anzupassen.
- *Präsentationssystem.* Wie auch immer die Produkt- oder Verwaltungsdaten tief im Inneren des Shop-Systems abgelegt sind – ihre Darstellung und die Art und Weise, wie diese Information aus den letzten Winkeln des Systems hervorgezaubert werden, ist eine eigenständige Funktionalität. Dabei sind Ausgangspunkt und Endpunkt dieses Prozesses eindeutig: Es gibt die Datenbank, an die SQL-Anfragen abzusetzen sind und zum anderen die endgültige HTML-Seite, die an den Kunden übermittelt wird. Zwischendurch kann der Weg jedoch sehr beschwerlich sein: üblicherweise werden HTML-Templates verwendet, welche aus einem HTML-Gerüst bestehen, in das unzählige Template-Variable (z.B. Intershop) oder Server-Side-Includes (z.B. Oracle's ICS) eingebaut sind. Letztlich steht hinter jeder dieser Erweiterung ein SQL-Zugriff. Wenn nun auch noch die HTML-Templates selbst in der Datenbank gespeichert werden und erst per SQL-Statement geladen werden können, wird der gesamte Zugriffsprozeß recht zäh. Betrachtet man also die Aufteilung des Shop-Servers zwischen Aufgaben der Kommunikation, Datenbankzugriffen und anderen Funktionen, so liegt der Hauptlastanteil eindeutig auf der Seite der Datenbank. Anbieter komplexer Shop-Systeme bieten vor allem in diesem Bereich flexible Konfigurationsmöglichkeiten, indem der Gesamtdatenbestand auf mehrere verteilte Server physikalisch verteilt werden kann.

- *Payment-Gateway*. Diese Software wird üblicherweise nicht von den Shop-Anbietern entwickelt, da hier ein anderes Know-How erforderlich ist, jedoch ist in viele der Shops-Systeme eine entsprechende Händler-Software bereits "gebündelt". Dies ist – aufgrund der Dominanz des amerikanischen Marktes – in der Regel das Cash-Register© von CyberCash. Im europäischen Raum hat neben CyberCash vor allem die Software X-Pay von Brokat besondere Bedeutung (XXX siehe auch ...). Payment-Module können zumeist über relativ einfach zu handhabende Command-Line-Schnittstellen eingebunden werden.
- *Werkzeuge*. Da der Online-Shop im Kern die Frage "Wie kommen meine Daten aus der Datenbank in die HTML-Seite" löst, gibt es inzwischen eine große Zahl Anbieter, die hier weiterhelfen. Das entscheidende Qualitätsmerkmal ist jedoch häufig folgende:
 - Die *Unterstützung des unkundigen Anwenders* beim Einrichten seines Shops. Hier werden unterschiedliche "Wizards" zur Datenübernahme der Produktinformationen, zur Konfiguration der Verwaltungsfunktionen sowie zur Interaktiven Gestaltung des Shops im Sinne eines Frage-Antwort-Spiels angeboten. Die damit verbunden Beispiel-Templates und sonstigen Ressourcen können durchaus eine Produkt-CD zu einem Drittel füllen...
 - Die *flexible Erweiterbarkeit* des Shop-Systems für Nicht-Standard-Anwendungen. Hier trennt sich Spreu von Weizen: nicht alle Shopssysteme verfügen auch softwaretechnisch über die klare Struktur, die im Hochglanzprospekt vorgeführt wird. Eine über Jahre und wechselnde Kundenanforderungen hinweg gewachsene "Spaghetti-Architektur" verhindert jedoch gerade eine flexible Erweiterbarkeit. Hier kann es bei der Anpassung des Systems schnell zu entscheidenden Verzögerungen kommen. Die erforderlichen Tools sind hier also im CORBA- und Active-X-Umfeld zu finden. Auch klar dokumentierte APIs und Java-Klassen zur Programmierung von Erweiterungen helfen dem Shop-Entwickler, das System kundengerecht anzupassen.

6.5.2 Allgemeine Architektur für Online-Shops

Wenn man durch die Hamburger Innenstadt schlendert, findet man tausende von Shops und Passagen. Jeders Geschäft besitzt eine individuelle Präsentationsschicht, ein eigenes Lagerhaltungsmodell und wählt nach eigenen Präferenzen aus, auf welche Weise Kunden ihre Ware bezahlen können. Jeder Shop setzt sich folglich aus einer Reihe von Basisfunktionen zusammen, die nach individuellen Kriterien ausgewählt und konfiguriert wurden.

Das gleiche gilt auf für einen Online-Shops. Die zuvor genannten Komponenten können, müssen aber nicht, Teil des Shops sein. Bei besonders spezialisierten oder innovativen Shop kann es sein, daß andere Bausteine hinzukommen, die man nicht als üblichen Bestandteil eines Ladengeschäfts auffassen würde.

Im folgenden gilt es daher weder darum, alle erdenklichen Komponenten eines Online-Shops aufzuzählen, noch die Architektur auf ein Mindestmaß zu reduzieren. Im Sinne einer Referenzarchitektur werden Zusammenhänge zwischen den wichtigsten Komponenten eines einzelnen Shops illustriert. Hierbei tritt die Shop-Software selbst als einzelnes Modul eher in den Hintergrund. Sie wird im Anschluß in ihre Einzelbestandteile aufgelöst werden.

Die Shop-Software bildet den Kern der Architektur, da sie die initiale Anlaufstelle für den Kunden darstellt. Dies gilt sowohl für den chronologischen Verlauf der Handelstransaktion als auch für das Weiterleiten von Anfragen die der Kunde mit seinem Web-Browser an den Server absetzt. Die Shop-Software setzt sich dabei aus unstrukturierten Inhalten wie Produktinformationen, Anbieterinformationen, redaktionelle Inhalte mit Unterhaltungs- und Informationscharakter sowie geschäftliche oder juristische Inhalte (AGBs, Datenschutz-Informationen). Die Kunst des Online-Shops besteht in der Integration solcher Inhalte mit den strukturierten Daten, welche die Shop-Software aus der Datenbank abfragt. Diese sind insbesondere Produktinformationen, Kundendaten, Preise und Rabatte, Kundendaten, Sitzungsdaten (z.B. die Verwaltung des Einkaufskorbs), etc. Wenn alle Geschäfte der Hamburger Innenstadt die gleiche Einrichtung besäßen, wäre es langweilig, mehr als eines aufzusuchen. Die redaktionelle Komponente spielt folglich eine wichtige Rolle bei der Individualisierung der immer wieder ähnlich gestalteten Datenbank-Inhalte eines Herstellers. Die Kunst, einen Online-Shop zu erstellen, endet folglich nicht mit dem Auswählen eines vorgegebenen Layouts vom Hersteller der Shop-Software. Eine flexible und effiziente Integration mit dem redaktionellen Teil des Gesamtsystems ist dringend erforderlich.

Gleiches gilt für die Integration von Werbung, wenn dies gefragt ist. Auch hier läßt sich die operative Schnittstelle zur Einblendung einer Banner-Bitmap serverseitig durch entsprechende Skripting-Technologien erreichen. Komplizierter wird es, wenn eine Personalisierung der Werbung erfolgen soll. Dann ist die Verwendung von Kundenprofilen erforderlich, die über die Shop-Software gewonnen wurden. Neben Kundendaten können jedoch auch noch Katalog- und Produktdaten als Parameter zur Auswahl des passenden Banners verwendet werden. Damit läßt sich sicherstellen, daß in der Rubrik „Finanzen“ bevorzugt Banner von Banken, Versicherungen etc. eingestreut werden. Dies bedeutet gleichzeitig, daß auch die Banner zur korrekten Zuordnung klassifiziert werden

müssen. Abgesehen von den Empfehlungen, die für einen bestimmten Banner sprechen, sollten noch weitere Aspekte, wie z.B. die der Fairneß bei der Auswahl einfließen. Wenn ein Werbekunde feststellt, daß sein Banner kaum angezeigt wurde (aufgrund der Verdrängung durch einen anderen), wird er zukünftig vom Schalten absehen.

Schließlich sind weitere Inhalte denkbar, die auf dem gleichen Empfehlungsmechanismus des Banner-Management beruhen können: So ist die Literaturempfehlung von Amazon.Com inzwischen legendär, bei der zu einem sekeltierten Buch eine Liste weiterer gezeigt wird, die andere Kunden zusammen mit dem angezeigten bestellen. Der Input für den Enpfelungsmechanismus kann entweder direkt aus den Profildaten des Web-Server ermittelt werden oder indirekt durch das Anlegen eines Data Warehouse.

Die Shop-Software führt kein isoliertes Dasein. Im „Back-End“ muß eine Anbindung an unterschiedliche Server erfolgen. Dies gilt insbesondere für die Anbindung an die Finanzbuchhaltung, die per Batch-Verfahren oder durch direktes Buchen beim Kauf erfolgt. Bei physischen Gütern ist bereits in der Informationsphase ein Zugriff auf den aktuellen Lagerbestand erforderlich. Und im Falle von Soft-Goods muß die Shop-Software die Download-Dateien sicher verwalten können, so daß nur autorisierte Kunden Zugriff erhalten.

Für den Prozeß des Bezahlens läßt sich schließlich ein Payment-Server einbinden, der von unterschiedlichen Herstellern (Brokat, CyberCash, NetLife etc.) angeboten wird. Hierbei muß sich der Shop-Betreiber genau überlegen, welche Zahlungsverfahren angesichts des Kundenkreises einzubinden ist.

Abb. XXX zeigt diese Softwarekomponenten eines Online-Shops in ihrem funktionalen Zusammenhang.

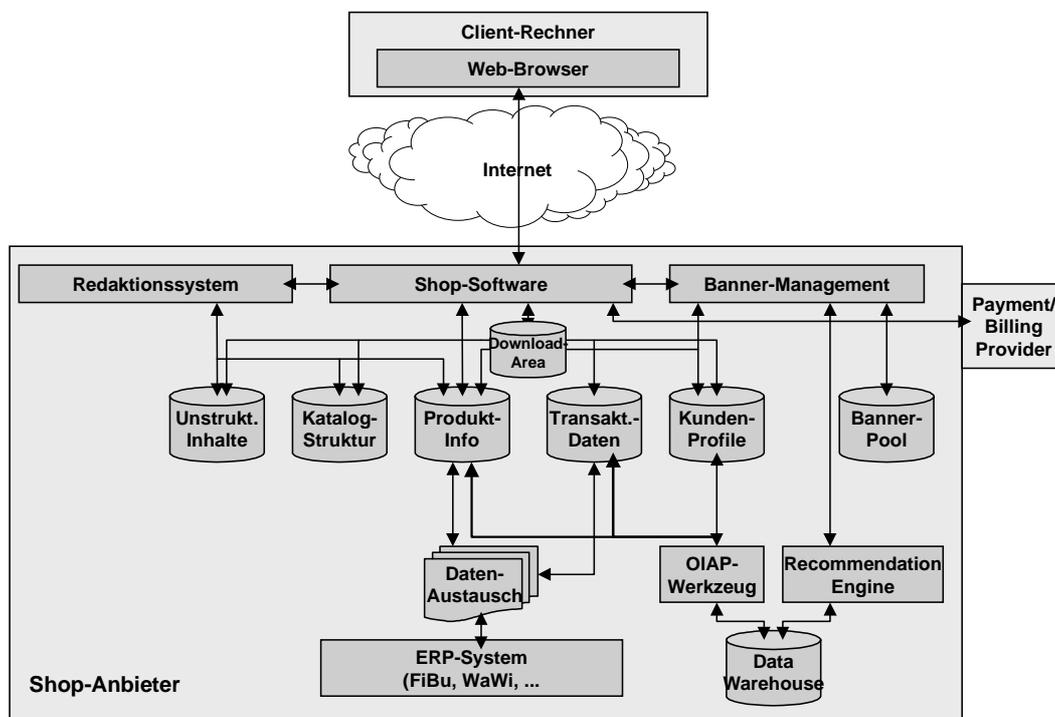


Abb. 23: Referenzarchitektur für Online-Shops

6.5.3 Beispiel: Intershop 3

Die Intershop-Software wird seit 1994 vom der Intershop AG in Jena entwickelt. Das Unternehmen gilt als eines der am schnellsten wachsenden Internet-Startups in Deutschland. Das Produkt Intershop 3 ist in verschiedenen Ausführungen zu erwerben: die Merchant-Edition stellt die Standardlösung für einen einzelnen Shop-Betreiber dar. Die Hosting-Edition ist als Mall-System einsetzbar und damit „mandantenfähig“. Jede Lizenz für einen Shop-Betreiber wird dabei einzeln berechnet. Am oberen Ende der Preis- und Leistungsskala steht die Enterprise-Edition, die nicht nur eine freie Konfigurierbarkeit der Datenbank erlaubt, sondern auch die Möglichkeit bietet, über serverseitige Plug-Ins das Shop-System flexibel zu erweitern. Im Gegensatz zur Enterprise Edition ist dem System bei anderen Version nur eine Laufzeitlizenz der Datenbank beigefügt, die keine Änderung am Schema zuläßt. Diese drastische Einschränkung spürt jeder, der ein umfangreiches Shopsystem bauen will.

Als Referenzkunden kann auf den ADAC-Online-Shop, Hewlett-Packard sowie Siemens verwiesen werden. Weitere Informationen lassen sich der Homepage von Intershop entnehmen (www.intershop.de).

Das wesentliche Merkmal von Intershop 3 ist seine leichte Handhabung auch für Programmierunkundige. Mit ein wenig NT- bzw. Unix-Administrationserfahrung läßt sich die Shop-Software, Datenbank und Demo-Software installieren. Einige Beispiel-Shops werden dabei gleich mitinstalliert. Die Definition des eigenen Shops erfolgt interaktiv über den *Store Design Wizard*, mit dem Graphiken und Layout definiert werden können. Dazu gehören auch Versandkostenarten, die Händleradresse sowie etliche Konfigurationsparameter für die Datenbank des Shopsystems. Nachdem nun die Gestaltung des Front-End abgeschlossen ist, sind in den folgenden Schritten der Katalog und Produktinformationen anzulegen sowie der Datenimport zu definieren. Auch hier stehen entsprechende "Manager" und "Wizards" zur Verfügung. Zuvor definierte Produkte können anschließend in den Katalog aufgenommen werden. Einzelne Produkte können dabei als Sonderangebot gekennzeichnet werden bzw. als Angebot für die Einstiegsseite in den Store. Die Verwaltungswerkzeuge sind im einzelnen:

- Im *Katalog Manager* wird die gesamte Artikelstruktur hierarchisch in Katalogen abgebildet. Der Administrator kann hier alle Rubriken eingeben, die dann im Katalog des Anbieters erscheinen (z.B.: Wohnzimmer-einrichtung → Couchgarnituren + Sessel + Lampen; Lampen → Tischlampen + Wandlampen etc.)
- Im *Produkt Manager* können neue Artikel angelegt oder bestehende geändert bzw. gelöscht werden. In der Artikelansicht lassen sich die Artikeleigenschaften und die Art ihrer Präsentation festlegen.
- Einige der zentralen Abläufe der Business-Administration werden im *Store Manager* verwaltet. Mit den in ihm enthaltenen Funktionen lassen sich Rechnungen und Lieferscheine generieren, die für die Bearbeitung einer Kundenbestellung notwendig sind. Innerhalb der Auftragsbearbeitung als Teil des Store Manager läßt sich der Status aller eingehenden Aufträge, offenen Rechnungen usw. überwachen.
- Der *Bestellungsmanager* erlaubt, den Warenbestand zu überwachen. Bestellvorschläge werden automatisch generiert, wenn die Lagerbestände zu stark absinken. Der Bestellungsmanager koordiniert sich mit dem
- *Lager Manager* wo die Verbuchung und Aufstellung aller Lagerbewegungen erfolgt. Dabei werden automatische und manuelle Buchungen unterschieden. Eine Buchung als Lagerabgang wird z.B. automatisch vorgenommen, wenn ein Lieferschein erstellt wird.
- Die Verwaltung der Kunden geschieht im *Kunden Manager*. Hier kann der Business Operator Kundendaten abrufen, neue Kunden anlegen oder Buchungen auf Kundenkonten vornehmen.
- Der *Service Manager* bietet Unterstützung bei allgemeinen Administrationsaufgaben und statistischen Aufgaben. Die Bereiche "Konditionen", "Statistische Auswertungen", "Produktstatistik", "Auswahllisten" und "Steuern" sind darin untergebracht.

Wenn ein Kunde einen Auftrag abgibt, druckt ein Sachbearbeiter des Anbieters einfach Rechnung und Lieferschein aus, überprüft die Zahlungsmethode und versendet die Produkte. Die verschiedenen Manager bringen ihre Daten automatisch auf den neuesten Stand. Zu diesem Zweck lassen sich verschiedene E-Mails konfigurieren, die der Shop-Server an den Kunden und den Shop-Betreiber sendet.

Realistischerweise werden Produktdaten nur in den seltensten Fällen manuell eingetragen. Viel wichtiger ist hier eine flexible Unterstützung des automatischen Updates. Zu diesem Zweck steht ein Sybase-ODBC-Treiber zur Verfügung, mit dem ein Massen-Update aus der Produktdatenbank des Unternehmens durchgeführt werden kann.

Als Zugabe erhält der Käufer des Intershop 3 noch das CashRegister von CyberCash, so daß auch die Anbindung an entsprechende Zahlungs-Gateways einfacher zu konfigurieren wird.

Intershop eignet sich durch seine benutzerfreundliche Einrichtung und Verwaltung des Online-Shops vor allem für kleine und mittlere Unternehmen, die über ein übersichtliches Produktangebot verfügen, welches sich in ein einfaches Kategoriensystem einordnen läßt. Als Gegenbeispiel lassen sich Produkte nennen, die nicht über ihre Kategorie, sondern über ihre Attributausprägung spezifiziert sind. Man stelle sich Amazon.Com vor, wenn sie ihren gesamten Warenbestand nach einer Taxonomie klassifizieren müßten. Hier ist auf jeden Fall die Unterstützung durch eine Suchmaschine sowie ein verfeinertes Taxonomiesystem erforderlich. Ersteres läßt sich bei der Enterprise Edition durch ein Plug-In (z.B. durch die Fulcrum Search Engine) realisieren, führt aber auch zu zusätzlichen Lizenzkosten.

Intershop wird ebenfalls im Beschaffungswesen eingesetzt, nämlich dann, wenn mehrere Abteilungen eines Unternehmens über eine zentralisierte Einkaufsabteilung ihren regelmäßigen Bedarf decken. Aufgrund des gebündelten Volumens ist die Beschaffungsabteilung nun in der Lage, mit Anbietern Umsatz- und Rabattvereinbarung zu treffen, die für einzelne andere Abteilungen nicht realisierbar wären.

Ein Manko liegt bei Intershop sicherlich in der Unterstützung von Soft-Goods, da ein flexibler Download- und

Billing-Mechanismus fehlt. Auch hier wird auf Plug-Ins verwiesen (z.B. ESD - Electronic Software Download), dies steigert jedoch auch die Komplexität des Systems erheblich. Eine Ausnahme stellt Linotype's FontExplorer@Web dar, für den jedoch die gesamte Funktion des Software-Download als Add-On entwickelt werden mußte.

Technologie

Im wesentlichen setzt sich der Intershop aus einer Sammlung von Perl-Scripts und einem RDBMS von Sybase zusammen.¹² Wie bei jedem Shop-System ist die "Middleware" – hier ist die Abbildung von Datenbankinhalten in HTML-Seiten gemeint – technologisch der interessanteste Bereich. Daher soll kurz auf Intershop's Hybrid-HTML (HHTML) eingegangen werden. HHTML sieht neben Standard-Tags weitere, proprietäre Variablen vor, die sog. TLE-Variablen (Intershops proprietäre *Template Language Extension*). Eine TLE-Variable kann beispielsweise das aktuelle Datum enthalten oder die Anzahl der Artikel im Warenkorb. Ferner sind auch einfache Kontrollstrukturen realisierbar, mit deren Hilfe der Programmierer beispielsweise durch die im Warenkorb befindlichen Artikel iterieren kann. Ein Beispiel für eine TLE-angereicherte HTML Seite und deren Endfassung nach Ersetzung der der Variablen ist in den folgenden Abbildungen gezeigt:

Abb. XXX: HHTML-Seite

Abb. XXX: Die HHTML-Seite, wie sie an den Web-Browser ausgeliefert wird

XXX Text zu Erläuterung.

Konfigurationsmöglichkeiten

Intershop nennt seine Konfiguration eine 4-Tier-Architektur, bei der also 4 Ebenen – bestehend aus Browser, Web-Server, Application Server und Datenbank – beteiligt sind.

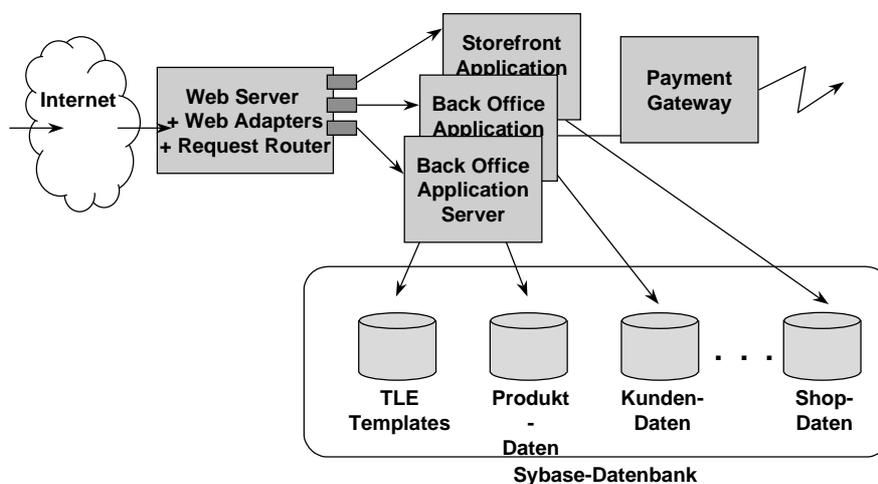


Abb. 24: Intershop-Architektur

Über das Internet eingehende Anfragen werden zunächst in Abhängigkeit von ihrer Portnummer an den betreffenden Application Server umgeleitet. Dieser kann auf einem anderen Rechner installiert sein. Bei hohen Lastanforderungen ist es zudem möglich, den Storefront-Server zu replizieren, so daß Shop-Anfragen auf mehrere Rechner verteilt werden können. Eine Administration des Shops ist ebenfalls über das Internet möglich, hier könnten ggf. Sicherheitsbedenken des Shop- oder Mall-Betreibers der Freischaltung entgegenstehen. Entsprechend sind im folgenden Konfigurationvarianten dargestellt, die den unterschiedlichen Anforderungsprofilen und Einsatzbereichen gerecht werden.

¹² Neuerdings wird auch Oracle 8 unterstützt.

1. Inhouse-Hosting

Bei dieser Variante betreibt der Händler seine Shopsoftware im eigenen Unternehmen. Alle Zugriffe von "draußen" werden von der Firewall gefiltert. Sie ist entsprechend konfigurierbar, so daß sie lediglich HTTP-Zugriffe auf den Shop-Rechner und über die dafür konfigurierte Portnummer zuläßt. Verwaltungsfunktionen werden ausschließlich über das Intranet realisiert, so daß hier keine Gefahr eines externen Angriffs besteht (Abb. XXX).

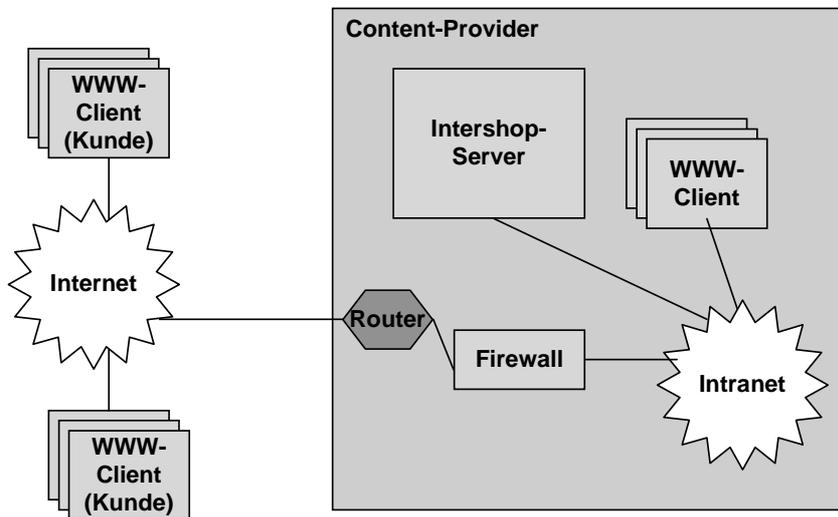


Abb. 25: Nutzungsvariante der Intershop-Software "Inhouse-Hosting"

2. Mall- und Abrechnungs-Provider

Die besondere Anforderung ist hier, daß sich ein Mall-System organisatorisch aus N+1 Betreibern zusammensetzt. Die N Shop-Betreiber – auch *Content Provider* genannt – möchten ihren Shop im eigenen Hause administrieren, gleichzeitig aber nahtlos in die Shopping-Mall eingebettet sein. Wichtig ist hier also eine Entkopplung aller Übergänge zwischen dem Mall-System und den einzelnen Shops. Dies gilt jedoch nur für die Produktinformation, denn der weitere Bestellvorgang und die Bezahlung soll schließlich wieder über den Mall-Betreiber abgewickelt werden. Folglich gilt es hier, Produktdaten, Shop-Daten und TLE-Daten beim Shop-Betreiber anzusiedeln und für die Abrechnung erforderliche Kunden- und Transaktionsinformation beim Mall-Betreiber (vgl. Abb. XXX)

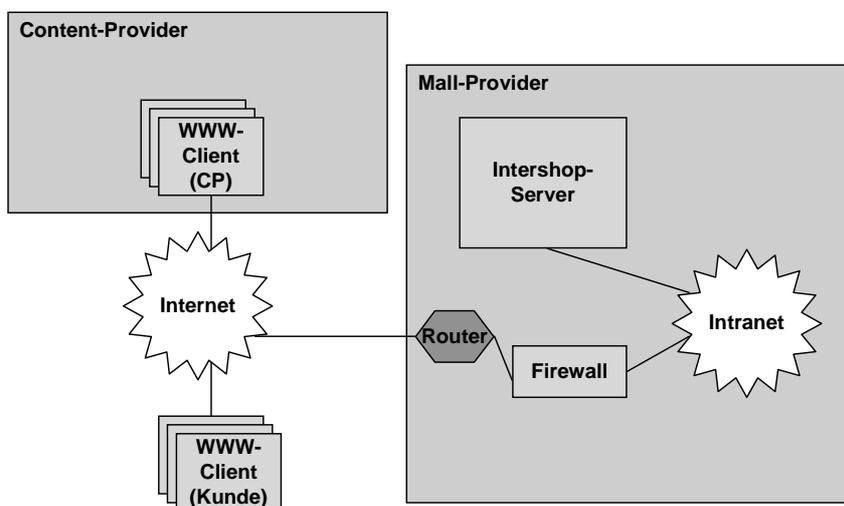


Abb. 26: Nutzungsvariante der Intershop-Software "Mall- und Abrechnungs-Provider"

3. Nur Mall-Provider

Im letzten Konfigurationsbeispiel ist die Aufgabe des Mall-Providers auf seine "Verteilerfunktion" reduziert. Hier erfolgt die Auslösung des Zahlungsvorgangs durch den Content-Provider. Abb. XXX zeigt eine Hybridform dieser Konfiguration, bei der die Transaktionsdaten beim Content-Provider gesammelt werden. Dieser kann beispielsweise eine Autorisierung für Kreditkartenzahlung durchführen, während die Abrechnung vom Mall-Betreiber realisiert wird. Dabei wird dem Mall-Betreiber Zugriff auf die Transaktionsdaten des Content-Providers verschafft (Abb. XXX).

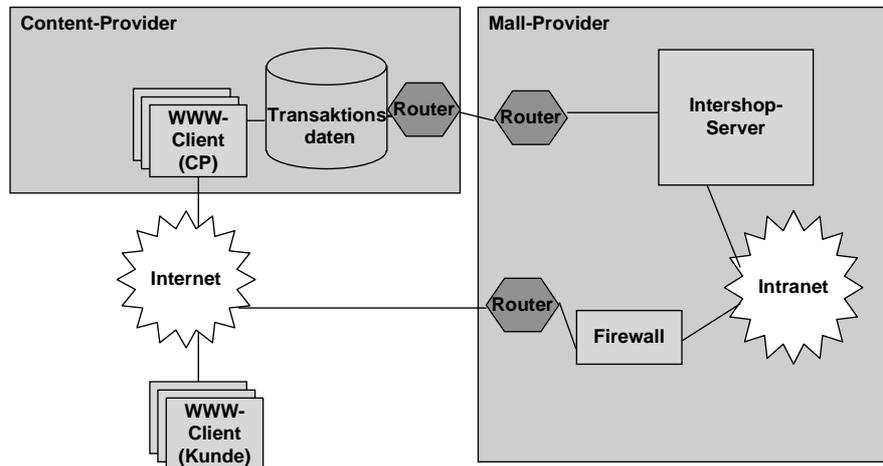


Abb. 27: Nutzungsvariante der Intershop-Software "Nur Mall-Provider"

Bewertung: Intershop 3

Von den analysierten Shop-Systemen zeichnet sich Intershop durch folgende Vorteile aus:

- Einfache Handhabbarkeit für einfache Shop-Anwendungen
- Umfangreiche Kundenbasis
- Integration der wesentlichen Zahlungsverfahren
- Vertretungen und Entwicklung in Deutschland mit Berücksichtigung nationaler Konventionen

Nachteilig ist allerdings die Beschränkung auf die reine Katalogfunktion mit angeschlossener Warenwirtschaft. Damit besteht eine grundsätzliche Ausrichtung auf Hard-Goods, d.h. es wird lediglich das Bestellen, jedoch nicht das Online-Ausliefern unterstützt.

Eine Intershop-Konfiguration wird sehr aufwendig, wenn die Anforderungen des Betreibers über die im Grundprodukt gegebene Funktionalität hinausgeht. Dies beginnt bei erweiterten Datenbankschemata für Kunden- oder Produktdaten über die Einrichtung eines flexiblen Katalogsystems mit beliebigen Einstiegspunkten und endet bei Features wie einer Suchmaschine, die als Add-on-Produkte von Dritten hinzugekauft werden müssen.

Des weiteren ist zu berücksichtigen, daß kurze Antwortzeiten bei der Katalognavigation besonders wichtig sind, damit der Kunde nicht aufgrund zu langer Wartezeiten das Interesse am Kauf verliert. Leider ist jedoch die Kombination Internet—TLE-Skripting—RDBMS häufig so langsam, daß ein spielerisches Navigieren und Auswählen schwerfällt. Dieser Nachteil gilt im allgemeinen für alle Shop-Produkte.

6.5.4 Oracle ICS

Der Internet Commerce Server (ICS) ging aus dem Apollo-Projekt von Oracle hervor und ist seit 1997 als Add-On-Produkt zur Oracle-Datenbank verfügbar. Er setzt auf Oracles Network Computing Architecture (NCA) auf und ist als Konfiguration von *Cartridges* des Web-Application-Servers von Oracle konzipiert. Die ICS-Cartridge bietet Programmierschnittstellen an, die dem CORBA-Standard IDL (Interface Definition Language) entsprechen.

Auch der ICS unterstützt das Hosting mehrerer Shops in einer Mall. Entsprechend der Abb. XXX erfolgt der Zugriff auf das Shop-System über Customer- und Merchant-Cartridges. Je nachdem, ob es sich um ein *Staging*- oder *Deployment-System* handelt, werden unterschiedliche Teile der Shop-Datenbank zugegriffen. Dabei wird jeweils unterschieden in "Static Data Owner" und "Transaction Data Owner". Beide Bereiche können unterschiedlichen Organisationen zugeordnet sein, so daß eine aktualisierte Shop-Version zunächst im Hause des Shop-Betreibers entwickelt und getestet und anschließend über ein "refresh" auf das Mall-System hochgeladen werden kann.

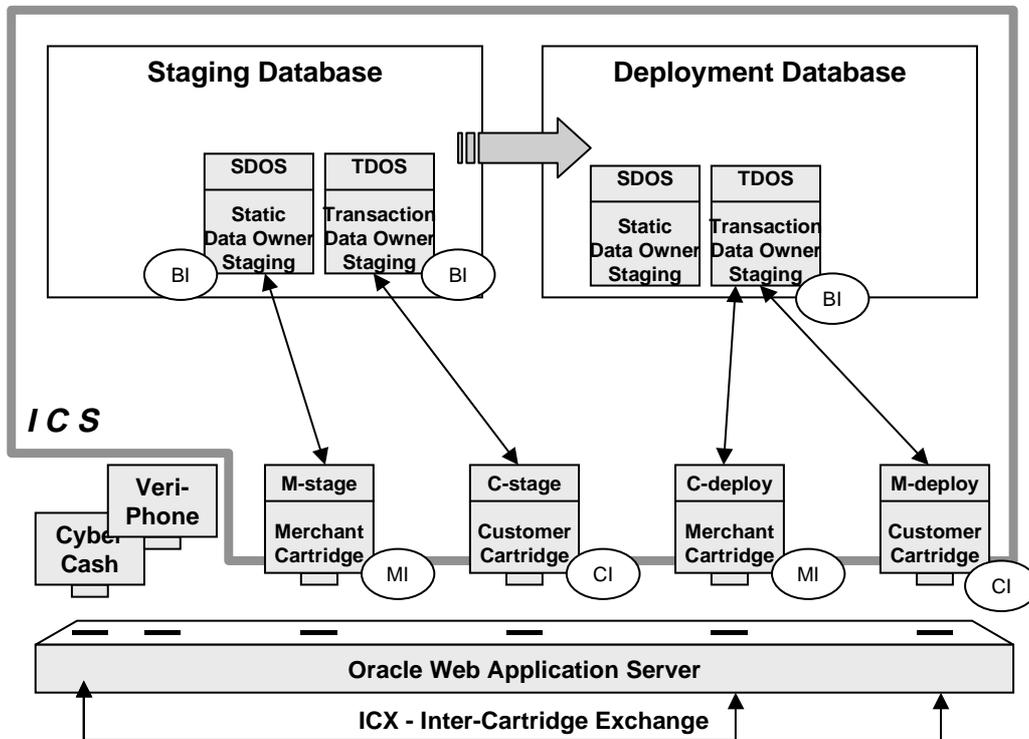


Abb. 28: Beispiele für die Erweiterung des Shop-Systems

OOOOS – Oracle's objektorientiertes Online-Shop-System

Der ICS folgt einem objektorientierten Ansatz, bei dem im Bereich der Administration und der Shop-Inhalte jedes Element als Objekt aufgefaßt wird. Das Einrichten eines Shops besteht damit in der Definition von Objekten und ihrer Beziehungen zu anderen.

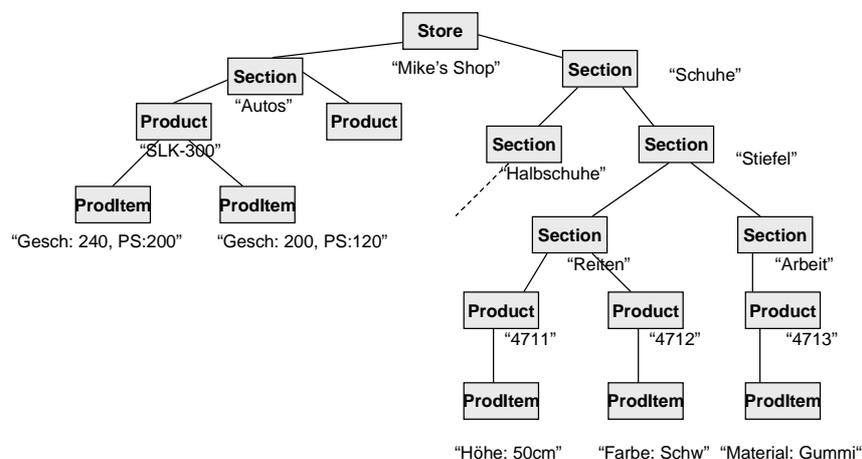


Abb. 29: Katalogschema beim ICS

Wichtig ist beim ICS die Unterscheidung in *Produkte* und *Attribute* (Product Items). Das Produkt definiert ledig-

lich die Kategorie, reicht aber noch nicht aus, um einen käuflichen Artikel vollständig zu spezifizieren. Produktvariationen korrespondieren dabei mit entsprechenden Ausprägungen der Attribute. Wenn es keine Variationen des Produkts gibt, ist trotzdem ein Dummy-Attribut erforderlich. Der Mercedes SLK aus der Sektion „Autos“ in Abb. XXX stellt beispielsweise ein Produkt dar. Erst in einer sinnvollen Kombination der Produkteigenschaften (z.B. Geschwindigkeit: 200, PS: 120) ergibt sich die volle Attributspezifikation der verfügbaren Variante.

Produkte lassen sich mit einer beliebigen Anzahl von Attributen und Referenzen kombinieren. Attribute können neben Standardtypen auch definierbare Wertemengen besitzen. Damit kann ein Attribut unabhängig definiert werden, so daß es für mehrere Produkte zur Spezifikation eingesetzt werden kann. Diese N:M-Beziehung zwischen Produkten und Attributen erfolgt auf der Ebene der Datenmodellierung des Katalogs.

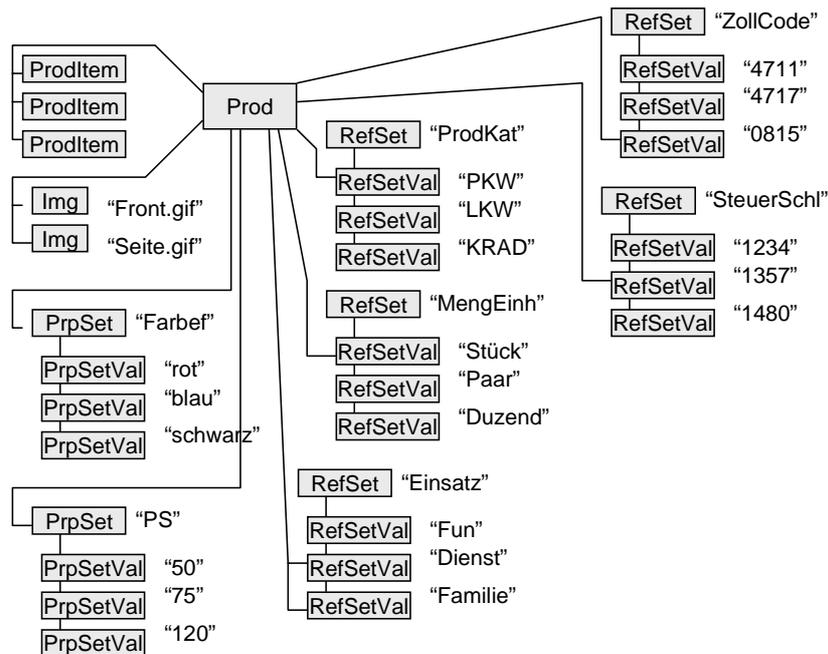


Abb. 30: Produkte, Product Items und Features beim Oracle ICS

Abb. XXX zeigt einige Attribute, die für ein Produkt definiert wurden. Attribute wie ZollCode, SteuerSchlüssel oder Mengeneinheit werden nicht nur für das abgebildete Produkt verwendet, sondern auch für beliebige andere aus diesem Grunde existiert eine Beziehung zum konkreten Wert eines solchen Attributs und nicht zum Attribut selbst. Beispielsweise gilt für das konkrete Produkt der Steuerschlüssel „1357“, der auch von anderen referenziert werden kann. Was die produktspezifischen Attribute betrifft, erfolgt der Verweis auf das Attribut, da erst beim konkreten Auswahlvorgang eine Wertausprägung gewählt werden kann.

Mit jedem Objekt (Produkt, Product Item, Section, Shopping Basket etc.) können beliebige *Contents* assoziiert sein. Contents sind Inhaltsobjekte, die im Browser des Benutzers visuell dargestellt werden können. Beispiele sind Icons, Logos, Banner, HTML-Templates etc. Aus der Schachtelung der Shop-Objekte von Store bis hinunter zum Product Item ergibt sich neben der Objekt-Hierarchie gleichzeitig auch die Schachtelungshierarchie der visuellen Darstellung.

Weitere Elemente der Shop-Architektur

Der ICS unterstützt eine Vielzahl weiterer Funktionen, die sich vor allem auch aus der einheitlichen Integration mit anderen Komponenten der NCA-Architektur ergeben. Zu diesen Funktionen zählt die Katalogverwaltung, die Verwaltung elektronischer Einkaufskörbe, die Bestell- und Zahlungsabwicklung, die Berechnung von Mehrwertsteuersätzen in Abhängigkeit von Bundesstaat (USA) bzw. Staat, die Konfiguration von Geschäftsregeln zur Automatisierung von Entscheidungsprozessen sowie die Integration mit der Auftrags- und Lagerverwaltung. Auf der Seite der Datenbank lassen sich Data-Warehouse- und Profilmanagement-Systeme zur Auswertung von Kundenprofilen einsetzen. Ähnlich wie bei anderen Produkten lassen sich zudem Rabatte und Rabattstaffeln für Kunden, Kundengruppen oder Artikel definieren.

Ein wesentliches Merkmal des ICS ist jedoch seine offene Architektur, dies es Drittanbietern erlaubt, über APIs

Zusatzmodule zu integrieren.

Auch für Produkte von Oracle gilt jedoch, daß die Einrichtung eines Shops oder einer Mall mit erheblichen Kosten verbunden ist: ein entsprechend komplexer Online-Shop kann dabei schnell bis zu einigen Millionen Euro an Investitionsvolumen erfordern. Aus diesem Grunde ist es sinnvoll, abschließend noch einmal auf das andere Ende des Preisspektrums zu schauen, um festzustellen, welche Leistung heutige Online-Malls fast zum Nulltarif bieten:

6.5.5 Shops für Jedermann

Wem es reicht, einfach nur mit einem eigenen Shop online zu sein, über den ein einfacher Katalog manuell verwaltet werden soll und der für Kunden zum Bestellen von Waren bereitsteht, kann einen solchen Service heute bereits zu monatlichen Gebühren zwischen Null¹³ und 50 Euro mieten. Anbieter wie www.mietshop.de oder www.strato.de bieten die Möglichkeit, vollständig über das Web den eigenen Shop einzurichten. Wer als kleines Unternehmen nur eine überschaubare Menge an Artikel zu pflegen hat, kann die wesentlichen Bestandteile des Shops selbst definieren:

- *Domain-Name.* Dieser wird meistens im Zusammenhang mit der Einrichtung eines e-Mail-Accounts oder einer Home Page gebucht.
- *Home-Page des Unternehmens.* Hierzu stehen Autorensysteme für Web-Inhalte zur Verfügung, die vom Anbieter genutzt werden können. Dabei lassen sich Staging-Varianten auf dem eigenen PC erstellen und anschließend auf den Mall-Server hochladen.
- *Einbindung redaktioneller Multimedia-Inhalte* (Grafiken, RealAudio- und RealVideo-Clips, Animationen und vorgefertigte serverseitige Funktionen).
- *Funktionen zur statistischen Auswertung.* Auch diese Funktion wird einem Shop-Mieter zur Verfügung gestellt.
- *Online-Katalog.* Der Katalog ist im Vergleich zu den zuvor dargestellten Produkten eher rudimentär. Varianten lassen sich häufig noch nicht definieren und zur Klassifikation des Warenangebots steht ein einfaches hierarchisches Kategoriensystem zur Verfügung.
- *Elektronische Einkaufskörbe* werden unterstützt, sogar bereits mit Berücksichtigung des Euro als alternatives Zahlungsmittel.
- *Orderfunktion.* Wenigstens eine Bestellung kann per e-Mail abgewickelt werden. Der weitere Prozeß muß dann im Unternehmen des Shop-Anbieters selbst abgewickelt werden. Dementsprechend kann auch keine Lagerbestandskontrolle durch den Shop durchgeführt werden.

Weitere Funktionen wie Kreditkartenzahlung, oder direkte Verbuchung der Käufe in der Finanzbuchhaltung sind ebenfalls nicht möglich. Dennoch stellen die neuen Billig-Malls eine interessante Möglichkeit für Privatpersonen und kleine Händler dar, die sporadisch Artikel online verkaufen möchten. Da ein solches Mall-System ohne nennenswerte Betriebskosten angeboten werden kann ist zu erwarten (1 Unix-Server, eine Mall-Lizenz zzgl. Entwicklungsaufwand für die Integration), daß ein solches Geschäft trotz der geringen monatlichen Gebühren bereits bei einigen hundert Shops wirtschaftlich betrieben werden kann.

6.5.6 Was ist noch zu beachten?

Junk-Orders

Junk-Orders sind leider eine Realität. Laut [EZI-Mailliste] liegt die Junk-Order Rate bei einigen Online-Malls der Anteil der Jux-Bestellungen bei bis zu 30% (Computerzubehör, CD, Bücher bei MyWorld) und sogar bei bis zu 60% in anderen Produktgruppen. Wahrscheinlich sind Donald Duck und Pipi Langstrumpf weltweite Umsatzspitzenreiter. Aber auch Schuldirektoren, Prominente oder einfach Nachbarn und Verwandte werden immer wieder gern als Opfer eines Junk-Orders eingesetzt. Damit ist verständlich, daß Online-Anbieter versuchen, möglichst an der Quelle derartige Fälle auszumerzen. So verfügt jedes größere Online-Unternehmen über eine nahezu

¹³ Wenn man einen e-Mail-Account beim Betreiber hat und von einer einmaligen Einrichtungsgebühr absieht.

vollständige Adressenliste deutscher Haushalte. Auch besonderes gefährdete Statusgruppen wie eben die Schuldirektoren sind häufig erfaßt. Beantragen diese Eintragung, erfolgt zunächst ein Rückruf des Anbieters beim „Opfer“. Und natürlich werden Negativlisten geführt, in denen die Ducks, Langstrumpfs und Mouses gespeichert sind. Diese Mechanismen werden auch ohne Internet bei allen Versandanbietern eingesetzt, so daß sie sich relativ leicht auf das Online-Modell anpassen ließen.

Die Angabe „normaler“ Opfer kann jedoch nicht vorab erkannt werden: Hier hilft zumindest eine e-Mail-Notifikation, falls eine Adresse angegeben wurde. Da es im MOTO-Bereich beim heutigen Service-Niveau üblich ist, daß einem Verbraucher das Rückgaberecht binnen einer gewissen Frist eingeräumt wird, ist ein nicht vermeidbarer Rest an fingierten Falschlieferungen nicht zu vermeiden. Erst mit der Einführung zuverlässiger Authentifikationsmechanismen (Signaturen nach dem DSig) kann eine Verbindung zwischen der Identität des tatsächlichen Bestellers und der Lieferadresse hergestellt werden.

Wer liefert was wie zuverlässig?

Mit zunehmender Anzahl an Shop verliert der Online-Markt an Transparenz. Analog zur Suchmaschine als „Neuer Intermediär“ bilden sich Online-Shopping-Führer heraus, die über ihr eigenes Katalogsystem Referenzen auf Shops verwalten. www.shop.de ist mit über 15.000 Einträgen das bekannteste Beispiel für solche Mehrwertdienste. Neben der reinen Sammlung von Referenzen wird die nächste Stufe in der Bewertung von Shops nach Qualitätsmerkmalen liegen. Shop.de erlaubt dabei die Bewertung des Shops nach einem Pauschalkriterium mit den Ausprägungen 1 (sehr gut) bis 5 (mangelhaft).

In den USA sind solche Rating-Services bereits heute schon Realität (siehe z.B. www.bizrate.com) und werden kontinuierlich verbessert. Ähnlich wie beim Amazon.Com Kunden angeregt werden, Rezensionen zu einem Produkt beizutragen, verwaltet BizRate Erfahrungsberichte von Shopping-Kunden. Dabei werden Rating-Kategorien vorgeschlagen, nach denen der Kunde den Shop bewertet. Als Resultat generiert BizRate eine Top-Ten-Liste sowie zu jedem Anbieter eine ausführliche Darstellung von Liefermodalitäten, Zahlungsbedingungen, Datenschutz-Policies usw. Insgesamt sind dies zehn Qualitätsmerkmale:

- der Preis,
- der Umfang des Produktangebots,
- die Produktinformationen,
- die Produktauswahl,
- die Gestaltung des Web-Angebots,
- die Navigation im Web,
- die Rueckgabemoeglichkeiten,
- die Auslieferung,
- die Beratung der Kunden und
- die Kundenbindung.

Das Geschäftsmodell von BizRate beruht übrigens nicht auf Werbeeinnahmen durch das Schalten von Banner, sondern wird von *Binary Compass Enterprise* betrieben, einem Unternehmen, das ein Verfahren zur Messung der Kundenzufriedenheit im Internet entwickelt hat, und entsprechende Analysen durchführt.

Erfahrungen mit Shopping Malls

Es kommt immer darauf an, was man will! Da die Investition zur Einrichtung eines Online-Shops zwischen einem Sonntagnachmittag und mehreren Millionen Euro kosten kann (Bertelsmann's hat sich BOL sogar 300 Millionen DM kosten lassen!), sind etliche Faktoren abzuwägen: Wer ist der Kundenkreis – Konsumenten oder Unternehmen? Wie sind die eigenen Artikel gestaltet – eher „Commodities“ oder sehr variantenreich und erklärungsbedürftig? Erfolgt die Bezahlung eher durch nationale oder durch internationale Kunden? Welcher Online-Umsatz ist zu erwarten? Wie volatil ist die Kundschaft und wie gut kann sie gebunden werden? Welche Bestandteile und Phasen der Kauftransaktion sind zu unterstützen? Wie soll die Integration mit dem „Back-Office“ erfolgen?

Diese Fragen lassen sich nicht pauschal oder durch die Definition einiger weniger Modelle beantworten. Hier ist zumindest eine eingehende Untersuchung bestehender Geschäftsabläufe erforderlich, wenn nicht sogar eine Ge-

schäftsfeldanalyse, bei der alle beteiligten Akteure auf dem betreffenden Marktsegment einbezogen werden.

Je nach dem Grad internationaler Aufmerksamkeit und der Attraktivität des Angebots kann es sein, daß der Shop jahrelang im Schneewittchenschlaf liegen wird oder daß er rasch durch schnellere Server und Datenbanken aufgestockt werden muß, da täglich einige tausend Bestellungen eingehen. Hierbei ist das Zusammenspiel aus Geschäftsmodell, Softwaretechnik, Logistik und Marketing ein Schlüsselfaktor. Bei einem Online-Shop mit schnell wachsendem Umsatz wird sich bald zeigen, wo der nächste Engpaß liegt. So mußte Amazon.Com einige Zeit leidvoll erfahren, daß das explosive Wachstum seines „Front-Ends“ im „Back-End“ – also bei der Bestellabwicklung und Auslieferung – nicht eingehalten werden konnte. Software und Hardware skalieren erheblich besser als die Lagerhalle, das Personal und die Lieferwagenkapazität des Kurierdienstes.

Viele Details lassen sich bestenfall an Fallstudien beschreiben – so war beispielsweise die Entscheidung Linotypes, für online gekaufte Font eine lebenslange Download-Garantie zu bieten, nicht nur aus Marketingmotiven bemerkenswert, sondern auch, da aufgrund der Kostenkalkulation und der „Download-Logistik“ getroffen wurde. Wie bereits bei der Diskussion der Internet-Ökonomie in Kapitel XXX dargestellt, gelten auch für Online-Shops veränderte Beziehungen zwischen den betriebswirtschaftlichen Einflußfaktoren. Somit ist vor der Einrichtung eines Online-Shops immer eine eingehende Markt- und Technologieanalyse erforderlich.

Lohnt sich ein Online-Shop?

Schließlich ist zu berücksichtigen, daß die Kosten einer hinreichen flexiblen Version von Intershop (der Enterprise Edition) bei 90.000 DM liegen. Desweiteren sind Kosten für Erweiterungskomponenten und die Hardware zu kalkulieren, die ebenfalls im Bereich einiger 10.000 DM liegen.

6.6 Customer Relationship Management

Steht der verfeinerte Apparat zur Profilbindung und -analyse zur Verfügung einmal zur Verfügung, liegt der nächste Schritt in der automatisierten und individualisierten Kundenbetreuung, amerikanisch-euphemistisch auch Customer Relationship Management (CRM) genannt. Dieser neueste Trend der Informationstechnik verspricht, mit chirurgisch exaktem Instrumentarium Kundenprofile, Marktanalysen und die eigene Produktpalette so zu schneiden, daß neue Marktnischen und Geschäftspotentiale erschlossen werden können.

Der Schlüssel zum CRM liegt dabei in der Ermittlung des Kundenverhaltens und der unmittelbaren Umsetzung dieses Wissens in eine Produktpalette, die dem individuellen Kunden direkt angeboten werden kann. Der Einsatz einer Internet-gerechten IT-Infrastruktur, die in der Lage ist, das Kundenverhalten vorherzusagen, soll Unternehmen gegenüber dem Wettbewerb einen erheblichen Service- und Effizienzvorsprung verschaffen.

Beispiele sind wiederum Empfehlungsmechanismen wie die Recommendation Engine von NetPerceptions (eingesetzt bei Amazon.Com) oder das anfangs erwähnte Grippemittel, dessen Auslieferung der Ausbreitung einer Grippewelle vorweg eilt. Als Wissensbasis für derartige Prognosen werden Zeitreihen historischer Absatzentwicklungen eingesetzt. Dazu muß dem System bekannt sein, welchen Verlauf eine Grippewelle üblicherweise nimmt, wieviele Bewohner in den betroffenen Gebieten leben usw. Diese Daten sind Unternehmen heute teilweise bekannt. Wenn sich sich zu verträglichen Kosten operationalisieren lassen, sind folglich neue Geschäftsmodelle möglich: Mit Endkunden könnte beispielsweise per „Service-Vertrag“ vereinbart werden, daß ein Medikament pauschal nach Hause geliefert wird, wenn die Wahrscheinlichkeit einer Infektion am größten ist. Ist der Kunde nicht betroffen, kann er es wieder zurücksenden. Im anderen Fall braucht er sich jedoch nicht zur Apotheke begeben. Sicherlich wird es Kunden geben, denen dieser Service möglicherweise sogar einen Aufpreis für die Lieferung ins Haus wert ist.

Auch bei diesem Beispiel spielen wieder einige der ökonomischen Parameter des Electronic Commerce – die Atomisierung von Information, Preisen und Mengen und die Verkürzung der Vertriebskette – eine wichtige Rolle beim CRM. Andere Beispiele des CRM könnten zu einer Personalisierung des elektronischen Einkaufskorbs führen: Wenn ein Kunde regelmäßig einen Kasten Wasser pro Woche beim Online-Supermarkt bestellt, könnte dieser beim nächsten Besuch automatisch den Einkaufskorb mit den entsprechenden Eintrag füllen. Das Kundenbedürfnis wird auch hier direkt aus dem Verhaltensprofil entnommen.

Andere Beispiele, die auf einer verfeinerten Profilbildung für Produkte und Kunden aufsetzen, sind proaktive „elektronische Verkaufsagenten“, die einem Kunden neue Music-Clips vorschlagen, die zu ihm „passen“ oder ihm aus der verwirrenden Vielfalt des Internet-Angebots ein multimediales Abendprogramm filtern, das sich aus Musik-, Film- und Print-Elementen zusammensetzt. Einem weniger ADSL-orientierten Kunde könnte ein solches

System ein Abendprogramm in der Großstadt schneiden – mit Vorschlägen für Abendessen, Kino, Clubs und einem Katerbrunch am nächsten morgen...

Zumindest in den USA ist zu erwarten, daß jedes konkrete oder abstrakte Objekt klassifiziert und profiliert werden wird, um einen automatisierten „Match on demand“ zu unterstützen. Manchmal fragt sich dabei der kritische Beobachter, ob das Individuum angesichts dieser omnipräsenten Profilbildung noch sein eigenes Profil erhalten kann?

Datenschützer erwarten bereits die nächste Konfliktwelle im Bereich des Profiling: Was passiert, wenn eine zu große Anzahl Kunden per P3P die Weiterverarbeiten von Profildaten untersagt, so daß das Instrumentarium CRM abstumpft? Werden Anbieter dann auf die erwartete Goldgrube verzichten? Besonders interessant sind Profildaten überhaupt erst, wenn sie in standardisierter Form zwischen Unternehmen ausgetauscht werden können. Um den Preis eines verschärften Wettbewerbs besteht in Zukunft erstmalig die Möglichkeit, die gesamte Bevölkerung zu erfassen. Eine restriktive Datenschutzgesetzgebung stünde dem nur im Wege...

CRM und Virtual Communities

Einerseits zielt CRM auf den individuellen Kunden ab, andererseits kann sich die entsprechende Software des Anbieters nicht um jedes Individuum isoliert kümmern. Durch die Bildung von Kategorien für Benutzer und Inhalte bzw. Produkte lassen sich ähnlich gestaltete Bedarfe zentral bedienen. So könnte die Ankündigung eines neuen Buches über ein entsprechendes System an all die Kunden propagiert werden, die als potentielle Käufer in Frage kommen. Wenn ein Anbieter nun bereits über diese Information verfügt, liegt ein Konsequenter Schritt im gegenseitigen „Bekanntmachen“ der Personen, da sie aufgrund ihrer Interessenverwandschaft bereits die Grundlage für eine Virtual Community besitzen. Eine selbsttragende Kunden-Community bietet neben dem Produkt des Anbieters als eigentlichem Inhalt die Möglichkeit, eine selbsttragende Aktivität zu entfalten, die den Anbieter in die Rolle des Moderators bzw. Betreibers schlüpfen läßt. Er profitiert dabei – ganz nebenbei – durch eine kostenlos verstärkte Sichtbarkeit bei weiteren Kunden. Wenn ich mich für ein Buch zum Theme Electronic Commerce interessiere, gehe ich häufig zu Amazon.Com, um dort kritiken zu lesen. Auch wenn es interessant ist – ich kaufe es nicht immer, aber häufig entdeckt man bei dieser Gelegenheit Neues, das man möglicherweise doch kauft. Genau dies ist *Virtual Community Management*.

7 Business-to-Business-Commerce

Wie bereits anfangs erläutert, unterscheidet sich der B2B-Commerce vom zuvor behandelten B2C-Commerce durch den vorherrschenden Zusammenschluß von Softwaresystemen und die damit verbundene Notwendigkeit, diese Systeme in einem veränderlichen Geschäftsumfeld flexibel zu halten. Handelstransaktionen laufen weniger schematisch ab als beim Online-Shop, da der Verhandlung von Konditionen und Verträgen größere Bedeutung beigemessen wird.

Während sich also Online-Shops das Internet als Präsentationsmedium zwischen Anbieter-Software und Privatkunde zunutze machen, ist die Beziehung Kunde-Anbieter beim B2B, technologisch gesehen, symmetrischer: Hier stehen sich zwei Softwaresysteme unterschiedlicher Anwender und von unterschiedlichen Herstellern gegenüber, die dennoch in gehaltvoller Weise miteinander kommunizieren sollen. Um dies zu erreichen, sind folgende Voraussetzungen zu erfüllen:

- Eine der wichtigsten Voraussetzungen ist dabei die *Interoperabilität* zwischen den beteiligten Softwaresystemen. Zu diesem Zweck stehen Middleware-Plattformen bereit, mit deren Hilfe, sich Unterschiede in Hardware und Betriebssystemen überbrücken lassen. CORBA erlaubt dabei beispielsweise die direkte Kommunikation zwischen Anwendungsobjekten, egal ob sie sich auf dem gleichen oder unterschiedlichen Rechnern verschiedener Hersteller befinden.
- Als nächstes ist für *Kohärenz* der Systeme zu sorgen, d.h., es ist ein standardisiertes Vokabular erforderlich, so daß die Software des Lieferanten den Bestellauftrag des Kunden „versteht“.
- Die *Softwaresysteme* müssen flexibel an neue Situationen und Geschäftsbeziehungen angepaßt werden können. Dies sollte idealerweise zur Laufzeit der Systeme – als ohne Manipulation des Quellcodes und ohne Unterbrechung des Betriebs erfolgen.
- *Workflow-Management*. Ein Geschäftsprozeß setzt sich aus mehr als nur dem Austausch von Daten zusammen. Wenn mehrere Unternehmen zusammenarbeiten wollen, so sind auch ihre internen Prozesse und Geschäftsregeln auf die Rollen abzubilden, die ein organisationsübergreifender Geschäftsprozeß definiert.
- *Verträge* helfen schließlich das, was sich technisch und ökonomisch im Geschäftsprozeß niederschlägt, auf der juristischen Ebene zu fixieren. Tritt ein Vertrag selbst als Softwareobjekt in Erscheinung, besteht zusätzlich die Möglichkeit, ihn als zentrale Definition des Workflows einzusetzen, wenn er sich in die „Sprache“ der Prozeßbeschreibung übersetzen läßt.

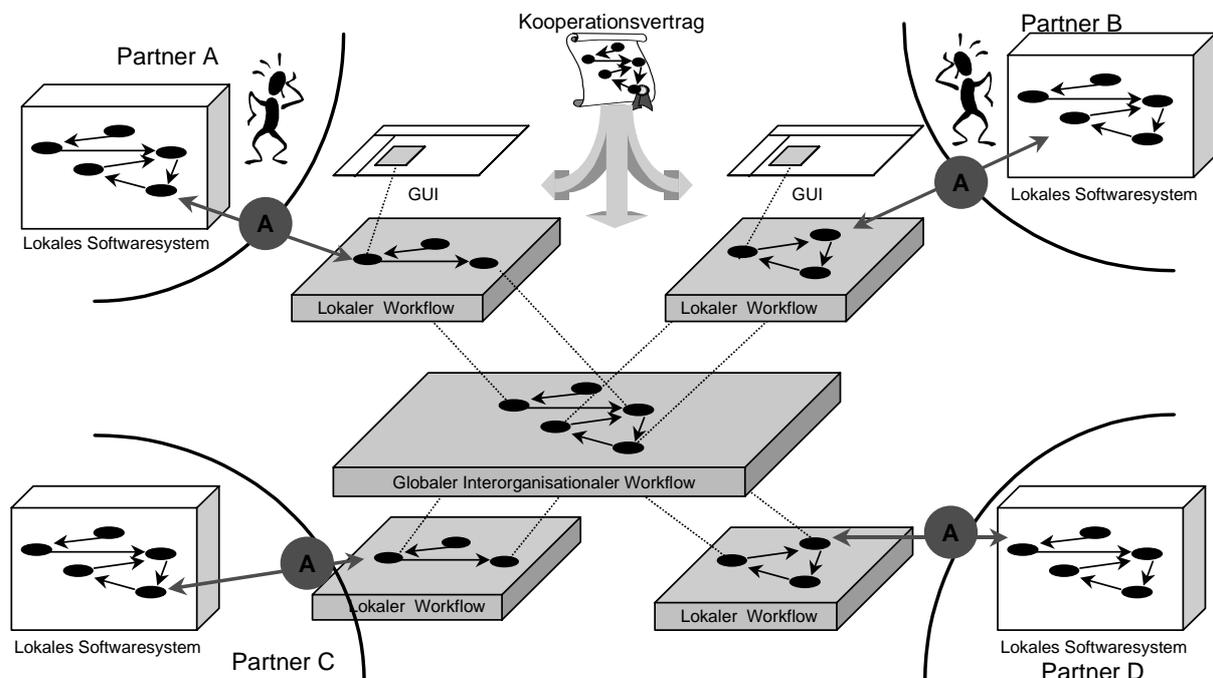


Abb. 31: Integrationsaspekte beim B2B-Commerce

Abb. XXX faßt die genannten Bedingungen zur Automatisierung des B2B-Commerce graphisch zusammen. Hier gilt es, über sog. *Adaptoren* (vgl. Abschnitt XXX weiter unten) die lokalen Softwaresysteme der beteiligten Ge-

schäftspartner so zu integrieren, daß ihre Schnittstellen und Prozesse in einheitlicher Form koordiniert werden können. Optional kann die dafür erforderliche Spezifikation als elektronisches Vertragsdokument aufgefaßt werden.

In den folgenden Abschnitten werden Technologien aufgezeigt, die helfen sollen, die Bedingungen einer optimalen Unterstützung des B2B-Commerce zu erfüllen.

7.1 Dokumentenaustausch beim Electronic Commerce

Wenn traditionell Handel betrieben wird, so ist damit ein reger Austausch von Daten verbunden: Ausschreibungsinformationen, Angebote, Aufträge, Lieferscheine, Rechnungen, Versandavise, Frachtpapiere, Stornierungen, Zahlungen und Bestätigungsschreiben – für jedes dieser Dokumente sind zwischen Auftraggeber und einer beliebigen Menge von Auftragnehmern Daten auszutauschen. Traditionell erfolgte diese Kommunikation per Post und auf Papier. Da jedoch diese Dokumente der jeweiligen Unternehmer nur geringfügig voneinander abwichen, war es mit der Einführung von Datenetzen grundsätzlich möglich, sie auch auf elektronischem Wege auszutauschen. Dies war die Geburtsstunde für EDI - dem elektronischen Datenaustausch (*Electronic Data Interchange*). Ziel der EDI-Standardisierung war die Schaffung eines einheitlichen Bestandes an Datenelementen mit einheitlicher Bedeutung für alle international beteiligten Unternehmen. Mit dieser Aufgabe konnte folglich nur eine internationale Organisation beauftragt werden, um eine entsprechende Vereinbarung international umzusetzen. Dies war im Falle von EDI die UNO.

7.1.1 Elektronischer Datenaustausch

EDI begann 1975 mit einer Publikation des Transportation Data Coordinating Committee (TDCC) darüber, welche Transaktionsdaten in verschiedenen Handelsabläufen in der Praxis genutzt werden. Anhand dieses Arbeitsmaterials wurde schließlich 1983 die Version 1 des EDI Standard von der ANSI, der US-Standardisierungsorganisation, verabschiedet. Damit wurden erstmalig generische Formate für den Datenaustausch im Handel festgelegt.

XXX Und EDIFACT?

EDI als Sackgasse?

Leider wurde das Ziel der Kohärenz nur bedingt erreicht. Obwohl EDI heute mehr denn je eingesetzt wird, sind dies zumeist nur Insellösungen, die sich um einen dominanten Spieler ranken. Die Deutsche Bahn AG betreibt beispielsweise ein EDI-gestütztes System zur Übermittlung von Transportaufträgen. Es läßt einen Durchsatz von bis zu 150.000 EDI-Nachrichten pro Stunde zu und dient der besseren Integration der Bahn AG mit ihren Kunden. Allerdings ist zu berücksichtigen, daß es sich hierbei nicht nur um Standardnachrichten handelt. Und genau dort liegt das Problem heutiger EDI-Systeme: Die Standardisierung von EDI erfolgt in der Praxis nach dem Machtprinzip und nicht nach einem Konsens. Der mächtigere Auftraggeber oder Kunde diktiert den kleineren Zulieferern oder Abnehmern sein Nachrichtenformat und Vokabular. Dies führt zu einer "Balkanisierung" der Nachrichtenformate, so daß am Ende eine blühende Industrie der *EDI-Konverter* entstehen konnte. Diese Software wird eingesetzt, um Nachrichten des einen Teilnehmers in solche des anderen umzusetzen. Das Umständliche an diesem Prozeß ist die Einbindung des Menschen in eine recht mühsame, fehleranfällige und letztlich kostspielige Arbeit, die bei Einigung aller auf einen einzigen Standard hätte vermieden werden können.

Leider bedeutet Standardisierung jedoch üblicherweise auch Verzögerung und diese ist bei EDI extrem hoch: Vom Vorschlag bis zur Umsetzung vergehen häufig mehrere Jahre, da beispielsweise ein neuer Vorschlag für einen Nachrichtentyp erst vom lokalen Gremium über die weltweit zentrale Standardorganisation wieder zurück in die nationalen, vertikalen und horizontalen Gremien fließt. So lange kann kein Unternehmen warten, das letztlich EDI nur deswegen einsetzen wird, wenn es einen Wettbewerbsvorteil bringt. Dieser muß sich jedoch besser innerhalb von Monaten als im Laufe mehrerer Jahre einstellen. Daher liegt das EDI-Dilemma darin, daß der Grad der Balkanisierung desto größer wird, je praxisrelevanter ein Nachrichtenformat ist.

Insbesondere für kleine Unternehmen kann der Einsatz von EDI eher höhere Kosten mit sich bringen als eine Kostensenkung: Falls sie nicht den von mächtigen Abnehmern diktierten Nachrichtenformaten gerecht werden, drohen diese, von weiteren Folgeaufträgen abzusehen. Da das Unternehmen häufig mehrere Abnehmer beliefert, kann es sein, daß dieses Anpassungsproblem in vielfältiger Form vorliegt. Will sich das kleine Unternehmen

nicht zu sehr an einen Kunden binden, droht es, in der Flut von Spezialformaten unterzugehen. Während der Anpassungsaufwand für den größeren Kunden marginal oder selbst noch im Falle eines einzigen Kunden sich für das kleine Unternehmen noch akzeptabel wäre, rechnet sich der jeweils erneut gegebene Anpassungsaufwand häufig bei zunehmender Kundenzahl nicht mehr. Für kleine und mittlere Unternehmen ist EDI damit sogar kontraproduktiv.

Abhilfe kann daher nur eine Hinwendung zu flexibleren Technologien schaffen. Insbesondere sind hier als "Stufe I" Internet und insbesondere das WWW als "Stufe II" zu nennen. Beim Internet würde zunächst die EDI-Nachricht in ihrem Originalformat per e-Mail übertragen werden. Obwohl dies banal klingen mag, ist es jedoch eine erhebliche Innovation gegenüber der heutigen Situation, in der VAN-Provider (Value-Added-Network) über Standleitungen und X.25-Protokolle ein proprietäres Netz speziell für den Austausch von EDI-Nachrichten betreiben. Für dieses Netz sind zumeist recht hohe Subskriptionsgebühren oder auch Gebühren auf Nachrichten- oder Volumenbasis zu bezahlen. Obwohl hier die Preise tendenziell fallen, gibt es noch Provider, die 20-30 Pfennig pro Kilobyte berechnen – und dies sowohl vom Sender wie auch vom Empfänger!

Obwohl nach wie vor einige Verfechter des VAN-basierten EDI stets die Nachteile des Internet ins Gefecht führen, setzt dieses sich zunehmend als technologisch beherrschbares, preiswertes, sicheres und zuverlässiges Medium durch. Daher seien hier kurz die wesentlichen Anti-Internet-Argumente genannt – und jeweils das Mittel zur Lösung der angeführten Problematik:

1. *Mangelnde Vertraulichkeit.* Dieser Punkt ist bereits gelöst durch die in Kapitel XXX erwähnten kryptographischen Methoden.
2. *Unkalkulierbarer Durchsatz.* Dies ist gerade bei EDI unproblematisch, da es keine Echtzeitanforderungen an das Kommunikationsnetz stellt. E-Mails können heute zuverlässig übermittelt werden.
3. *Möglichkeit des „Spoofing“ (Maskerade).* Gelöst durch Authentisierungsmechanismen.
4. *Keine direkte EDI-Unterstützung.* Aktuelle Standards zur MIME-Einbettung sind vorgeschlagen und befinden sich in der Umsetzung. Dabei ist insbesondere RFC#1767 zu nennen, der das MIME-Applikationsformat für die EDI-Standards EDIFACT und X12 festlegt.
5. *Sicherheits-Verwaltungsfunktionen.* Diese sind in Browser oder e-Mail-Tools fest integriert.
6. *Schlüssel-Management.* Hierzu dienen die in Abschnitt XXX diskutierten Zertifizierungsdienste.
7. *Keine Verarbeitungsfunktionen für kryptographische Funktionen.* Auch diese sind heute fest in Browser oder e-Mail-Tools integriert. Zudem läßt sich Software wie z.B. PGP leicht auf Anwendungsebene integrieren.
8. *Problematische Verbindungen zwischen VANs und dem Internet.* VANs werden gar nicht erst benötigt. Stattdessen erfolgt die Kommunikation über das "Extranet", also den Bereich des Unternehmensnetzes, den sich Geschäftspartner gegenseitig zugänglich machen.

Einige Unternehmen bieten schon die EDI-Anbindung über das Internet an, wie z.B.: GEISCO (www.getradeweb.com) heute bereits in 8 Ländern.

EDIFACT

Obwohl EDI häufig mit EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) gleichgesetzt wird, kann dem nicht zugestimmt werden: Während sich EDI grundsätzlich dem standardisierten Datenaustausch zwischen Geschäftspartnern widmet, schreibt EDIFACT bestimmte Nachrichtenformate und deren Semantik konkret vor. EDIFACT findet seine größte Akzeptanz in Europa, während in den USA der ANSI X12-Standard das mit EDIFACT nicht interoperable Gegenstück darstellt. Darüber hinaus wurden von der UN sog. Standardnachrichten (UNSM – United Nations Standard Messages) festgelegt, die branchenunabhängig universell einsetzbar sein sollen. Das in diesen Nachrichten ausgedrückte Wissen um Geschäftsbeziehungen und die dazu erforderlichen Datenformate stellt ein außerordentliches Gut für die Realisierung von Electronic-Commerce-Systemen dar. Aus diesem (und nur aus diesem) Grunde sollte EDI besondere Aufmerksamkeit geschenkt werden.

Das grundlegende Strukturierungsmittel ist bei EDI das *Datenelement*. Eine Rechnung würde beispielsweise die einzelnen Rechnungspositionen als Datenelemente enthalten. Datenelemente können zu *Datenelementgruppen* und diese wiederum miteinander oder auch mit einzelnen Datenelementen zu *Segmenten* zusammengefaßt werden. Eine *EDI-Nachricht* besteht aus mehreren Segmenten. Schließlich können selbst Nachrichten innerhalb einer *Verbindung* weiter zusammengefaßt werden zu *Übertragungsdateien*.

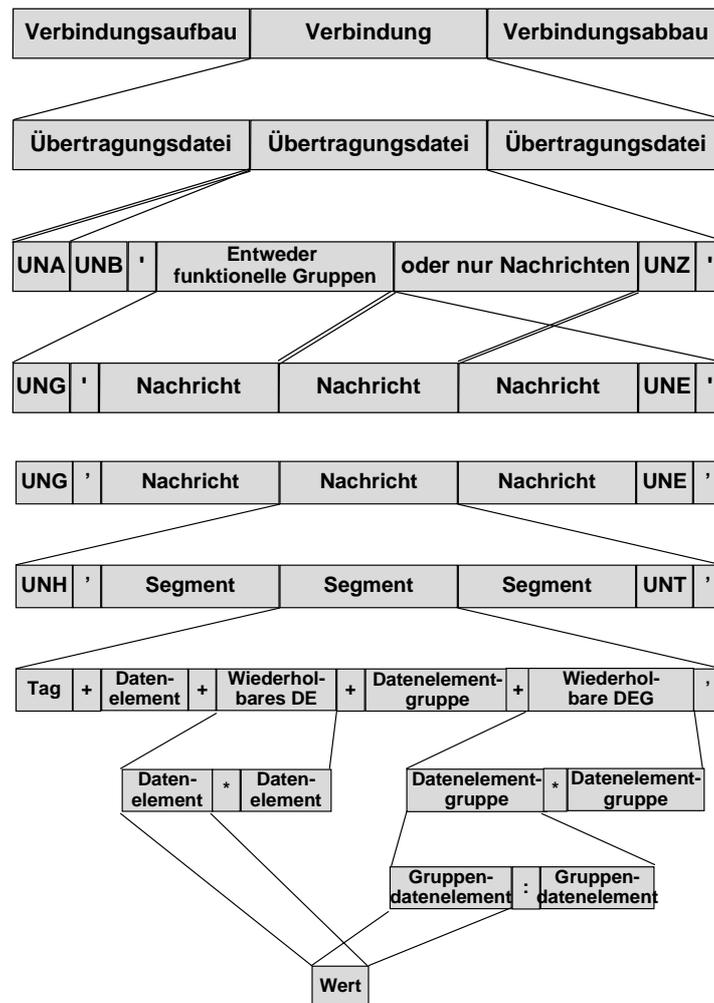


Abb. 32: Schema von EDI-Nachrichten

EDIFACT-Standards definieren über EDI hinausgehend, welche Datenelemente notwendig, optional oder bedingt sind und legen fest, ob, wie oft und in welcher Reihenfolge bestimmte Datensegmente wiederholt werden können. Für jede EDI-Nachricht wird eine Felddefinitionstabelle geführt. Die Felddefinitionstabelle eines jeden Datensegments legt wiederum das Schlüsselfeld fest. Ferner sind folgende Vereinbarungen und Regeln enthalten:

- Datenformat
- Struktur von Datensätzen variabler Länge
- Datenfelder und Gruppen von Datenfeldern
- Datentypen
- Wertebelegung
- Zeichensätze
- Schlüsselwörter und Trennzeichen
- Nutzungsindikatoren
- Wiederholungsregeln
- Auslassungsregeln

Die Abbildung XXX zeigt einen exemplarischen Geschäftsprozeß, der vier Rollen umfaßt, die je nach konkreter Instanzierung von unterschiedlichen Unternehmen eingenommen werden können. Jeder einzelne Datentransfer entspricht dabei einer EDI-Nachricht. Hierbei ist deutlich erkennbar, daß die tatsächliche Organisation des vollständigen Prozesses weit über die Definition einzelner Nachrichtentypen hinausgeht: Das Beziehungsgeflecht der Akteure kann dabei beliebig komplex sein, einzelne Nachrichten sind optional, während andere in Abhängigkeit von bestimmten Regeln mehrfach auftreten können.

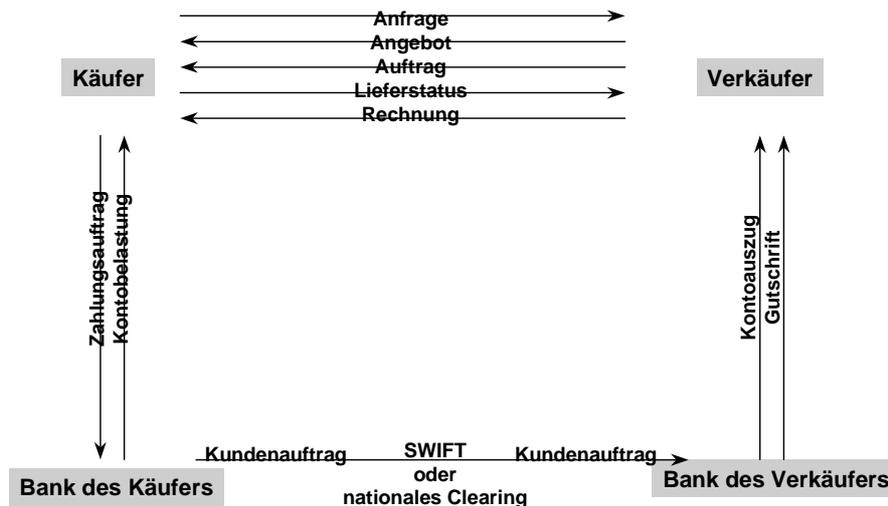


Abb. 33: Vollständiger Geschäftsprozeß und beteiligte EDI-Nachrichten

EDI wurde ursprünglich für den Datenaustausch mit Hilfe von Telex-Geräten entwickelt. Daher liegen Nachrichten in einem Zeichenformat vor, das weder die Einbettung von Binärdaten, noch die von Softwarekomponenten erlaubt. Der heutige Austausch von Java-Applets oder die Kommunikation zwischen CORBA-Objekten hat EDI technologisch somit um Jahrzehnte angehängt.

Um EDI von seinem Manko der Beschränkung auf den Austausch von Textdateien zu befreien wurden verschiedene Versuche unternommen, um EDI herum weitere Aspekte der interorganisationalen Kooperation zu erfassen. Folgende Beispiele sind dabei relativ bekannt:

- Open EDI
- Objektorientiertes EDI
- Universal EDI
- XML/EDI

Auf den letzten Ansatz wird jedoch erst nach der allgemeinen Einführung von XML weiter unten eingegangen.

7.1.2 Open EDI

Open-EDI kann als Vision der Standardisierungsorganisationen ISO und IEC für die Zukunft angesehen werden. Das Open-EDI-Referenzmodell (ISO/IEC-Standard Nr. 14662 verfügbar auf <http://www.iso.ch> unter JTC1/SC32/WG1) nutzt UML als Sprache zur Modellierung organisatorischer Zusammenhänge und Objekte.

Open-EDI ist ein generischer Ansatz, der Unternehmen in der kurzfristigen und preiswerten Etablierung von Geschäftsbeziehungen unterstützt. Durch die Nutzung von Standard-Szenarien für den Handel sollen Eintrittsbarrieren für Unternehmen, die am elektronischen Datenaustausch partizipieren wollen, reduziert werden. Für diese Standardszenarien werden Werkzeuge und Dienste zur Verfügung stehen, die eine rasche Implementierung unterstützen. Die Open-EDI-Vision sieht vor, daß, wenn sich die Partnerunternehmen auf ein Szenario geeinigt haben, dessen Implementierung standardkonform ist, keine weiteren Vereinbarungen zwischen ihnen getroffen werden müssen.

Open-EDI kann zwischen beliebigen und beliebig vielen Organisationen innerhalb einer Branche, aber auch über Branchen hinweg eingesetzt werden. Die ausgetauschten Daten sind nicht auf Standardtypen beschränkt, sondern können auch Binärdaten umfassen. Das Open-EDI Referenzmodell wird unabhängig von Inhalten, unternehmensspezifischen Prozeduren oder technischen Infrastrukturen entwickelt.

Im Gegensatz zum "klassischen" EDI, erweitert sich die Sichtweise beim Open-EDI von der Festlegung von Datenformaten zur Spezifikation von Geschäftsprozessen. Folglich steht neben der Definition von Datenobjekten jetzt auch die der Geschäftslogik selbst im Vordergrund – soweit dies überhaupt standardisierbar und formalisierbar ist. Die Verbindung mehrerer EDI-Nachrichten zu Sequenzen, die Definition von Prozessen und Regeln sowie die Festlegung von Rollen innerhalb komplexer Kommunikationsbeziehungen sind die wesentlichen neuen Aufgaben des Open-EDI.

Geschäftsprozesse lassen sich in ihre Basisprozesse zerlegen oder umgekehrt zu komplexeren zusammensetzen. Die Sprache UML wird dabei benutzt, um Geschäftsprozesse hinsichtlich ihrer Anforderungen, Use Cases, Klassendiagrammen sowie Aktivitäts- und Zustandsdiagrammen zu modellieren. Für den Datentransfer werden XML-Dokumente verwendet. Dabei nutzt das System Repositories, in denen XML-DTDs verwaltet werden.

Die Hoffnung besteht beim Open-EDI darin, daß durch die Verwendung von UML als objektorientierte Modellierungssprache eine wesentliche formalere und präzisere Beschreibung von Geschäftsprozessen möglich sein wird und damit Softwarebausteine für die EDI-Kommunikation als "Fertigprodukte" zur Verfügung gestellt werden können.

Es wird angestrebt durch die Entwicklung von Standard-Geschäftsszenarien wählbare Schablonen bereitzustellen, für denen Benutzung die Geschäftspartner im Rahmen einer Handelstransaktion keinen speziellen Rahmenvertrag abschließen müssen ("Trading Partner Agreements") [Wrig91].

Dabei werden zwei Sichtweisen hervorgehoben:

- Die *Business Operational View* (BOV). Hier wird die Semantik von Datenobjekten und Nachrichten festgelegt sowie Regel für Geschäftstransaktionen. Diese umfassen Vereinbarungen und gegenseitige Verpflichtungen, die mit einer Transaktion verbunden sind. Bezogen auf den Geschäftsprozeß in Abb. XXX würde nach dem Open-EDI eine Schablone für das verwendete Ablaufmodell zur Verfügung stehen, die den beteiligten Akteuren Rollen zuweist und den Ablauf koordiniert.
- Die *Function Service View* (FSV) hebt unterstützende Dienste hervor, indem sie sich eher auf softwaretechnische Fragen bezieht. Dazu zählen Möglichkeiten zur Auslösung, Durchführung und Überwachung von Handelstransaktionen, Benutzungsschnittstellen, Sicherheitsmechanismen etc. Dabei soll Open-EDI rückwärtskompatibel zum "klassischen" EDI bleiben.

7.1.3 Interaktives EDI

Heute lohnt sich EDI nur bei hohen "Economies of Scale", d.h. bei einer intensiven Nutzung, die die hohen Investitionskosten für beide Seiten rechtfertigt. Inzwischen gibt es jedoch verschiedene Projekte und Standardisierungsbestrebungen, bei denen versucht wird, eine EDI-Nachricht mit Hilfe eines Web-Browsers zu visualisieren (als sog. *E-Forms*). Dies gilt sowohl für eingehende als auch für zu versendende Nachrichten. Es können drei verschiedene Ansätze unterschieden werden, um dies zu erreichen:

- Nutzung *dynamischer HTML-Dokumente* auf der Serverseite. Hierbei kann eine Nachricht an den Benutzer eines Browsers gelesen werden, indem sie serverseitig mit Hilfe von Scripts generiert und vom Benutzer geladen wird. Diesem bleibt nur die Möglichkeit, die Seite zu sichern oder auszudrucken. Umgekehrt kann ein Benutzer über den Browser und ein HTML-Formular EDI-Nachrichten mit Werten füllen und absenden. Dabei sind die HTML-Formulare jedoch statisch in der Weise, daß Wiederholungsgruppen nicht hinzugefügt werden können. Dies kann nur über Folgeseiten realisiert werden, so daß die gesamte Web-Programmierung schnell unübersichtlich wird und nur mit hohem Wartungsaufwand gepflegt werden kann. Eine Bestellung läßt sich beispielsweise nur eingeben, indem zunächst ein Hauptformular mit gemeinsamen Formularfeldern ausgefüllt wird und anschließend für jeden Posten eine eigenes Formular zu laden ist.
- Nutzung von *Java-Applets* auf der Clientseite. Java bietet die Möglichkeit, flexible Formulare zu generieren, so daß auch Wiederholungsgruppen in Formularen als Listen flexibel verwaltet werden können. Des weiteren hat der Programmierer die Möglichkeit, Eingabeüberprüfungen vor Ort durchzuführen. Die Konvertierung in eine EDI-Nachricht kann unmittelbar durch das Applet erfolgen, so daß dem Server eine Nachricht im EDI-Format übertragen werden kann. Allerdings ist der Code zur Konvertierung und Visualisierung individuell zu programmieren, d.h. der Aufwand ist noch wesentlich höher als bei den dynamischen HTML-Seiten.
- Nutzung von *XSL*. Schließlich bietet sich die Möglichkeit, Informationen zur Visualisierung einer EDI-Nachricht an eine XML-DTD zu koppeln, so daß man beim Laden der Nachricht als XML-Datenstruktur automatisch einen Verweis auf die betreffenden XSL-Regeln erhält (siehe Abschnitt XXX zu XML). Diese XSL-Definition ist für jeden Nachrichtentyp standardisiert und könnte im Internet zentral verfügbar gemacht werden. Hier wäre nur einmal eine Java-Software zu entwickeln, die für beliebige EDI-Nachrichtentypen die Visualisierung spezifiziert. Alles weitere würde über die DTD gesteuert werden.

Auch wenn durch Web-Integration EDI-Nachrichten ad hoc empfangen oder versendet werden können, ist damit noch keine Integration der Software gegeben. Weder die Konvertierung der ausgetauschten Nachricht in das lokale Format, noch die Einbettung in komplexe Geschäftsprozesse ist damit gelöst. Hierin besteht jedoch das eigentliche EDI-Problem, so daß die Frage nach dem Datenaustausch zwischen der lokalen Anwendungssoftware und dem Java-Applet im Web-Browser noch offen bleibt.

Interactive EDI kann also nur zur Einbindung von Personen in den Dokumentenfluß eingesetzt werden. Hier fragt man sich jedoch berechtigterweise, warum dann überhaupt EDI über das Internet erforderlich ist, wenn doch über das Web und in Verbindung mit Server-Side-Scripting die Datenein- und -ausgabe direkt auf der Datenbank des Anbieters erfolgen kann.

7.1.4 Universal EDI

Universal EDI ist eine weitere Bestrebung, die versucht über die Standardisierung von Nachrichtenformaten hinauszugehen, um vollständige Geschäftsprozesse definieren zu können. [XXX Quellen finden!] Unterschieden werden hierbei technische und logische Aspekte der Kommunikation und Kooperation zwischen Geschäftspartnern. Beim Universal EDI werden daher vier Kommunikationsebenen unterschieden:

- *Geschäftspraktiken.* Auf dieser obersten Ebene legen Unternehmen Regeln zur Interaktion mit anderen Geschäftspartnern fest. Beispielsweise zählt dazu, wann eine Bestellung beim Lieferanten erfolgt oder wann eine Mahnung geschrieben wird. Die erforderlichen Ereignisse, die zur Durchführung einer Interaktion nötig sind, werden auf dieser Ebene beschrieben. Gleiches gilt auch für die erforderlichen Geschäftsprozesse.
- *Geschäftsprozesse.* Hier werden Abfolgen von Ereignissen und Datentransfers festgelegt, die zur Durchführung eines Geschäftsprozesses erforderlich sind. Grundlegende Zusammenhänge zwischen Datentypen und auszuführenden Aktivitäten seitens der Partner sind durch den Geschäftsprozeß beschrieben.
- *Informationsmodell.* Diese Ebene entspricht dem klassischen EDI. Es wird die Struktur und Bedeutung ausgetauschter Daten festgelegt.
- *Technologie.* Unterstützende Dienste zur Übertragung, Verarbeitung und Speicherung der ausgetauschten Daten werden auf dieser Ebene definiert. Zu kann beispielsweise eine CAD-Anwendung festgelegt werden, die vom Geschäftspartner empfangene Nachrichten verarbeitet, wenn es sich um den Austausch technischer Produktbeschreibungen handelt.

Diese vier Ebenen sind erforderlich, um alle Details einer Kooperation zwischen Unternehmen zu beschreiben. Um beispielsweise eine Flugreservierung durchzuführen, muß zunächst bekannt sein, welche wer als Dienstleister in Frage kommt und welche Optionen bestehen. Erst dann können auf der nächsten Ebene die Schritte des Reservierungsprozesses durchlaufen werden. Eine Ebene tiefer werden dann Dokumente und Formulare eingesetzt, die sich aus den Spezifikationen des Geschäftsprozesses ergeben. Am Ende selektiert die Universal-EDI-Software die Technologie zur Übertragung oder Verarbeitung der Daten – also beispielsweise Fax, e-Mail oder EDI.

Wollen zwei Unternehmen miteinander in Verbindung treten, führen ihre EDI-Systeme ein Art „Handshake“ durch, ähnlich der Art und Weise wie Modems die Übertragungsparameter zu Kommunikation verhandeln. Während Modems feststellen, welches die höchste gemeinsame Übertragungsrate ist, versuchen die EDI-Systeme abzustimmen, auf welchen Ebenen sie sich auf der Basis welcher Geschäftsprozesse in Verbindung setzen können. Dabei versucht Universal EDI, die Interoperabilität der Partner zu verbessern ohne gleichzeitig die Wettbewerbsfähigkeit der Unternehmen durch zu starke Nivellierung einzuschränken. Insbesondere für Routine-Kooperationen z.B. im Gesundheitswesen, bei Reisebuchungen, im Beschaffungsbereich oder bei der Kommunikation mit Behörden ist eine solche Schematisierung nicht notwendigerweise wettbewerbshemmend.

Die Entwicklung von Universal EDI

Universal-EDI-Standards werden in zwei Phasen, der *Geschäftsanalyse* und der *Entwicklung von Standards* festgelegt. In der ersten Phase werden alle Informationen gesammelt, die zur Festlegung des Standards erforderlich sind:

- Identifikation der Teilnehmer,
- Definition von Rollen,
- Rahmenbedingungen der Umwelt werden in Form von Regeln festgelegt,
- Informationen, die lokal vorliegen,
- Informationen, die in Dialogen ausgetauscht werden.

Als Ergebnis liegt dann eine Spezifikation der Komponenten vor, deren Kommunikation sich anschließend simulieren läßt. Anschließend werden Prozeß- und Datenmodelle eingesetzt, um die Kommunikation zu strukturieren. Beispielsweise könnte sich ein Prozeßmodell für die Reservierung aus Einzelaktivitäten vom Typ *Vakanzprüfung*

und *Reservierung* zusammensetzen, wobei erstere beliebig oft durchgeführt werden kann, bevor eine Reservierung erfolgt. Das Datenmodell legt dabei die Datenobjekte fest, die im Prozess ausgetauscht werden. Nachdem das Daten- und Prozeßmodell definiert wurde, wird es in einem Repository abgelegt.

Anschließend erfolgt nach dem Universal-EDI-Modell die Entwicklung des Standards. Hierbei werden semantische Dateneinheiten definiert, die zunächst das abstrakte Verständnis spezieller Geschäftsdaten reflektieren. So könnte beispielsweise „Stückliste“ eine semantische Dateneinheit sein, die in Branchen wie Industrie, Tourismus oder Dienstleistung auf unterschiedliche Weise verfeinert wird. Mit Hilfe von Metainformationen können zudem weitere Optionen oder Bedingungen festgelegt werden, welche die Integration dieser Informationen mit anderen Einheiten steuern.

Neben einer Strukturierung von Datenobjekten werden auf der Ebene von Prozessen und Nachrichten auch Alternativen festgelegt, auf die sich die Universal-EDI-Software zur Kooperation ebenfalls per „Handshake“ einlassen könnte. Einige weitere Elemente, die einen Universal-EDI-Standard ausmachen, schließen die Entwicklung des Standards ab. Das Resultat soll damit am Ende

- eine eindeutige Spezifikation des Standards,
- die Eliminierung weiterer Anforderungen für Implementationsrichtlinien,
- wiederverwendbare Standardkomponenten, sowie
- eine flexible Unterstützung des Nachrichtenaustausches

liefern. Insbesondere soll Universal EDI virtuellen Unternehmen damit den erforderlichen „Kitt“ zu flexiblen Integration ihrer Geschäftsprozesse – auch über Branchengrenzen hinweg – liefern.

Zusammenfassung zum "Universal EDI"

Es ist nicht abzustreiten, daß zukünftig beim B2B-Commerce in stark wachsendem Maße Daten elektronisch ausgetauscht werden und daß eine umfassende Standardisierung die Effizienz und Flexibilität von Geschäftsbeziehungen in gleichem Maße verbessern wird, wie das WWW und e-Mail die zwischenmenschliche Kommunikation weltweit erleichtert.

Entsprechend der anfang angeführten Voraussetzungen, ist zudem eine ganzheitliche Unterstützung der Unternehmenskooperation nötig. Universal EDI versucht daher – ähnlich dem Open EDI – durch detaillierte Geschäftsanalysen diesen Prozeß vollständig zu erfassen, um in einer anschließenden Phase daraus Standards abzuleiten.

Bemerkungen zu EDI

EDI hat ein Trägheitsproblem: Es zielt auf die Standardisierung von Prozessen und Informationen ab, die auf bilateraler Ebene im einem Bruchteil der Zeit harmonisiert werden können. Die Zeit, die jedoch für einen globalen Standard erforderlich ist liegt, wie bereits gesagt, bei mehreren Jahren. Selbst wenn die gesamte Industrie heute noch einmal auf der grünen Wiese ihr Geschäft aufnehmen könnte, würden viele behaupten, daß sich kein einheitlicher Standard in allen Wirtschaftsbereichen durchsetzen würde. Dies liegt weniger an der Beschränkung von EDI auf Datenstrukturen, sondern vielmehr an der Ökonomie der Standardisierung. Sie erfordert zuviel „Overhead“ für das einzelne Unternehmen. Außerdem ist die Identifikation wiederverwendbarer Bausteine und Nachrichtentypen ein langwieriger Filterprozeß, der sich praktisch nur im Zyklus aus Vorschlag-Test-Bewertung-Verbesserung-Vorschlag entwickeln kann. Folglich dürfte die Harmonisierung von EDI auch die nächsten Jahrzehnte andauern, wenn sie in der gewöhnten Weise fortgeführt werden würde.

Eine Chance zur Besserung verspricht allerdings mit XML eine der jüngeren Entwicklungen im Internet. XML, das als „HTML der Zukunft“ gepriesen wird, bietet weitaus flexiblere Möglichkeiten zur feinkörnigen Standardisierung von Nachrichtenobjekten. Doch bevor wir uns XML zuwenden, sollte auch HTML als Alternative in Betracht gezogen werden.

7.1.5 HTML als Alternative?

Seit einigen Jahren gibt es nun mit HTML einen weiteren "Nachrichtenstandard", der für eine wachsende Gemeinschaft von Nutzern eingesetzt wird. HTML-Dokumente sind die "Protokolldateneinheiten" des HTTP. Sie werden individuell vom Anbieter einer Web-Site gestaltet und mit Inhalt gefüllt. Dabei existiert für die Semantik

einer "HTML-Nachricht" keinerlei Vorschrift, lediglich ihre Darstellung ist über die Standardisierung der Auszeichnungssyntax durch das W3-Konsortium festgelegt. Auch wenn es hierbei hin und wieder zu abweichenden Implementierungen kommt, ist dennoch der gemeinsame Nenner aller "HTML-Implementierungen" (im Sinne von Web-Browsern) im Vergleich zum EDI beachtlich hoch. Bezogen auf das Standardisierungsziel, eine einheitliche Auszeichnungssprache zu definieren, war damit HTML nicht nur erheblich erfolgreicher als EDI, sondern sicherlich neben der technischen Vernetzung des Internet einer der Hauptfaktoren für dessen explosives Wachstum in den letzten Jahren. Es ist durchaus denkbar, daß sich auch EDI ähnlich hätte entwickeln können, wenn dem "Expertenteam" entsprechende Zeit und "Exklusivität" zur Einigung gewährt worden wäre.

Natürlich hinkt der Vergleich zwischen EDI und HTML ein wenig, da es sich um völlig unterschiedliche Anwendungsbereiche handelt: EDI standardisiert Struktur und Semantik von Nachrichten, jedoch keine Präsentation, während HTML Struktur und Präsentation, jedoch keine Semantik standardisiert.

Sieht man sich jedoch heutige Web-Sites im Internet an, fällt auf, daß neben der Präsentation zunehmend strukturierter, dynamischer Inhalt zu finden ist. Dies gilt nicht nur für Produktkataloge, sondern fast für den gesamten redaktionellen Inhalt einer Web-Site (aktuelle Nachrichten, White Papers, Projektinformationen). Während man vor zwei bis drei Jahren noch den Inhalt einer geplanten Web-Site eher visuell beschrieb, werden heute zunehmend Werkzeuge zur Datenmodellierung der Inhalte eingesetzt. Früher waren es statische HTML-Seiten, die von der Festplatte unverändert an den Browser transportiert wurden; heute dient HTML als dünne, dynamisch generierte Präsentationsschicht, die die äußerste, für den Anwender sichtbare Schicht einer komplexen Softwarekonfiguration ausmacht.

Mit dieser Entwicklung besteht nun zunehmend die Anforderung, Web-Inhalte erstens auch semantisch zu strukturieren und zweitens diese Struktur nach Möglichkeit zu standardisieren, was der Zeilsetzung des EDI entgegenkommen würde. Da diese inhaltliche Struktur jedoch unabhängig ist von ihrer Darstellung (man kann eine Produktinformation sowohl als "flaches" HTML-Dokument präsentieren als auch als hierarchisch strukturiertes, editierbares Datenobjekt), ergeben sich folgende Probleme: Wie lassen sich aktuelle Innovationen in den Bereichen "Präsentation", "Auszeichnungssyntax" und "Semantik" gleichzeitig standardisieren, ohne

- gegenseitige Beeinflussung der Standards,
- "Balkanisierung" der jeweiligen Standards und
- untragbare Verzögerungen hinzunehmen?

Die aktuelle Lösung lautet "divide et impera": Teile die drei Schwerpunkte in unabhängige Ebenen, erlaube deren unabhängige Standardisierung, aber erzwinge ein Minimum an Einheitlichkeit, welches ein Optimum im Trade-off einerseits zwischen der Maximierung standardisierter Elemente und der Standardisierungsgeschwindigkeit andererseits zuläßt. Wieder einmal ist es die Höhe des gemeinsamen Nenners, von der der Gesamterfolg der Standardisierung abhängt.

SGML

An dieser Stelle tritt ein weiterer Standard auf die Bühne: *SGML* (Standard Generalised Markup Language) d.h. eine standardisierte, verallgemeinerte Auszeichnungssprache. Diese Sprache wurde 19XX von Charles F. Goldfarb entwickelt und fand ihren Einsatz bisher hauptsächlich im Bereich von Redaktionssystemen. SGML erlaubt die Definition von Grammatiken für strukturierte Dokumente. Dies zerfällt in zwei Ebenen, die *Dokumententypdefinition* (DTD) und die eigentliche Auszeichnung des Dokuments:

1. Die DTD legt die Syntax fest, also die Regeln, nach denen ein zu ihr konformes Dokument konstruiert werden kann. Ein Dokument, welches eine Abteilung repräsentiert, könnte also konstruiert sein aus einem Leiter (mit dessen Angestellteninformation), der Adresse der Abteilung sowie einer Liste von Angestellteninformationen für alle weiteren Mitarbeiter. Eine Angestellteninformation setzt sich ihrerseits wieder aus einer vorgeschriebenen Menge an Datenelementen zusammen. Auf der Ebene des SGML-Standards wird einheitlich die Syntax für diese Konstruktionsregel festgelegt. Damit sind SGML-konforme Softwarekomponenten in der Lage, unterschiedliche DTDs zu verarbeiten. Umgekehrt kann jeder Anwender seine eigene DTD festlegen.
2. Für die Auszeichnung des Dokuments werden - wie von HTML gewohnt - *Marken* verwendet. Im Gegensatz zu HTML haben SGML-Marken jedoch keine festgelegte Bedeutung (bei HTML steuern sie die Darstellung von Dokumenten im Web-Browser). Eine SGML-Marke dient lediglich als "Phänotyp" des in der DTD vorzufindenden "Genotyps". Aus der Verbindung zwischen DTD in konkretem SGML-Dokument kann nun mit Hilfe eines Verifizierers abgeleitet werden, ob das Dokument gültig ist, d.h. mit seinen Elementen den Strukturierungsregeln der DTD entspricht. Wie bei der DTD reduziert sich der eigentliche Standard von SGML lediglich auf die Syntax der Marken, von denen erwartet wird, daß sie sich aus einem Klammerpaar <...>, ei-

nem Markennamen sowie einer optionalen Liste von Attributen zusammensetzen. Diese Regel gilt für jedes SGML-Dokument, unabhängig von seiner Bedeutung und der verwendeten Namen.

- Als dritte Komponente eines SGML-Dokuments kann eine entkoppelte Präsentationsebene verstanden werden, welche die gegenüber HTML verlorene Festlegung der Dokumentenvisualisierung ermöglicht. Als Co-Standard zu SGML wurde daher *DSSSL* (Document Style Semantics and Specification Language, sprich: "Dissel") entwickelt. DSSSL ist eine algorithmisch vollständige Skriptsprache, anhand derer für jede SGML-Marke eine Regel festgelegt werden kann, die ihre Visualisierung steuert. Beispielsweise würde die HTML-Marke <H1>, die einen Text als Überschrift der höchsten Gliederungsebene definiert, etwa so aussehen:

XXX Beispiel DSSSL??? Wichtig: Textbezug in Vorzeile!!!

Ein spezieller SGML-Anwender hatte nun das Problem, mit anderen Fachkollegen (Physikern) Informationen auszutauschen, die jeder für sich im Internet zur Verfügung stellte und die gleichzeitig in flexibler Form miteinander als verteiltes Hypertextsystem über das Internet verbunden werden konnten. Dieser Tim Berners-Lee vom schweizer CERN entwickelte eine DTD, welche als erste Version von HTML im Jahre 1989 das Licht der Welt erblickte. HTML ist also ein in SGML definierter Dokumententyp. Und als anwendungsspezifischer Typ besitzen seine Marken auch entsprechende Bedeutung, wie wir sie von allen HTML-Dokumenten her gewohnt sind. Mit diesem Schritt wurde der gemeinsame Nenner der Standardisierung erheblich höher gesetzt als bei SGML: jetzt ist nicht mehr nur die Markensyntax, sondern auch die Semantik der Marken sowie die Präsentation vorgeschrieben. Dies war zunächst nicht grundsätzlich schlimm, da HTML gerade die einheitliche Präsentation zum Ziel hatte. Als HTML jedoch in den letzten Jahren immer weniger der Aufgabe gerecht werden konnte, auch *Inhalte* jenseits der Präsentation in einheitlicher Form zu repräsentieren, betraten zunehmend neue Standards die Bühne. Dabei sind zwei Strömungen zu erkennen:

- *Ad-hoc-Standards*, die im Rahmen des eingeschränkten Korsetts von HTML versuchen, zusätzliche Semantik unterzubringen.
- Die *Extended Markup Language*, von dem sich die Gemeinschaft der Web-Designer, der Tool-Entwickler und letztlich auch der Electronic Commerce- und EDI-Anwender ein hohes Maß an Synergie versprechen.

Als Vertreter der ersten Kategorie ist beispielsweise die <META> Marke im HTML zu nennen, die als "Hintertür" zur Unterbringung von Meta-Information zum Dokument dient. Damit bleibt der Inhalt dieser Marke spezialisierten Gremien überlassen, die sich z.B. mit Fragen zur Dokumentenklassifikation oder der Bewertung von Web-Sites (wie z.B. PICS, Abschnitt XXX) beschäftigen. Diese Standards sind eher pragmatischer Natur - es ging primär um die rasche Nutzbarmachung dieser Zusatzinformation.

Wie bereits erwähnt, spielt sich jedoch das Leben einer Web-Site immer weniger auf der Präsentationsebene ab. Stattdessen stehen Fragen der Datenbankanbindung und der redaktionellen Unterstützung und Integration in das Unternehmen im Vordergrund. Die Problemstellung läßt sich dabei wie folgt zusammenfassen: Gefragt ist die Einfachheit von HTML mit der Mächtigkeit von SGML, jedoch ohne die Einschränkung der ersten und die Komplexität der letzteren.

XML (Extended Markup Language) kann hier als gesunder Kompromiß verstanden werden. Es ist eine Untermenge von SGML, insbesondere blieb die Möglichkeit der Grammatikdefinition erhalten. Es kann gleichzeitig als eine Reduzierung von HTML aufgefaßt werden, da – wie bei SGML – den ausgezeichneten Komponenten eines Dokuments keine Visualisierung vorgeschrieben wird. Gleichzeitig entsteht durch diese Lücke gegenüber HTML der Bedarf nach einem DSSSL entsprechenden Co-Standard zu XML. Dieser Standard existiert unter dem Namen *XSL* (Extended Style Language). Ebenso wie beim DSSSL wird die Visualisierung von XML-Dokumenten über Regeln festgelegt. XSL ist gegenüber DSSSL hinsichtlich seiner Mächtigkeit ein wenig reduziert, mit dem Vorteil, daß es effizienter implementierbar und im WWW schneller einsetzbar ist. Die Skriptsprache basiert auf ECMAScript, der standardisierten Form von Netscape's JavaScript.

Die Standardisierung von XML und XSL spiegelt den Status quo im Bereich der Auszeichnungssprachen wieder. Etliche Hersteller bieten inzwischen Redaktionswerkzeuge (Poet, XXX), Datenbanken (Poet, Oracle), Programmierbibliotheken (DOM, SAX, XXX), Import/Export-Bibliotheken und sonstige Werkzeuge (XXX, Software AG) für XML an. XML wird heute bereits von einer unzähligen Zahl an Unternehmen unterstützt. Gleichzeitig findet sich eine Vielzahl von Projekten bei Anwendern, die XML nicht mehr nur in Verbindung mit dem WWW einsetzen, sondern für den internen Datenaustausch *im* und zunehmend auch *zwischen* Unternehmen. Genau an dieser Stelle befinden wir uns also wieder auf dem Weg zurück zum Ausgangspunkt des Themas "Dokumentaustausch beim Electronic Commerce": dem EDI. Auch bei XML ist die Anzahl an Standardisierungsaktivitäten kaum mehr zu überschauen:

- Bibliotheken nutzen XML-Erweiterungen zur Klassifikation von Literatur sowie allen über das WWW zugänglich gemachten Informationsressourcen (RDF, Dublin Core)

- Innerhalb des Web-Konsortiums (W3C) wird ein Standard definiert, welcher erlaubt, eine Qualitätsbewertung von Web-Sites und HTML-Seiten in einheitlicher Form vorzunehmen (als XML-Neuaufgabe von PICS).
- Profilinformationen für Benutzer werden so standardisiert, daß sie zwischen Anbietern austauschbar sind und - quasi im "Kollektiv" - vollständigere Information aus diesen Daten ermittelt werden kann (Open Profiling Standard sowie P3P).
- Schließlich ist die Integration von XML und EDI in Richtung XML/EDI zu nennen, die wahrscheinlich das größte Potential birgt. Hierbei ist die Abbildung von EDI-Nachrichtentypen auf DTDs sicherlich der einfachere Teil der Aufgabe. Der lukrativere liegt jedoch in der Entschlackung von EDI durch Nutzung preiswerter und flexibel konfigurierbarer XML-Werkzeuge. Dabei ist zu erwarten, daß gegenüber EDI langfristig die finanzielle Eintrittsschwelle zur Nutzung und zur Anpassung zwischen Unternehmen gesenkt wird. In Verbindung mit einer weiteren Standardisierung von Austauschprozessen für Geschäftsdokumente (vgl. z.B. *OFX*, Open Financial Exchange oder das *OTP*, Open Trading Protocol) könnte sich im internationalen Handel genau das vollziehen, was bisher im WWW nahezu perfektioniert wurde: Vollständige Markttransparenz. Damit kann XML und seine Verwendung bei Elektronischen Datenaustausch als ein Mittel zur weiteren Annäherung an das ökonomische Modell des vollständigen Konkurrenzgleichgewichts aufgefaßt werden.

7.1.6 XML

XXX HIER IST NOCH EINIGES ZU BEARBEITEN!!!

XML als Metasprache

- XML soll im Internet verwendet werden.
- XML soll ein breites Spektrum von Anwendungen unterstützen.
- XML soll kompatibel mit SGML sein.
- Es soll einfach sein, Programme zu schreiben, die XML-Dokumente verarbeiten.
- XML-Dokumente sollen für Menschen lesbar und klar verständlich sein.
- XML-Dokumente sollen leicht zu erstellen sein.
- Der Entwurf soll formal und präzise sein.

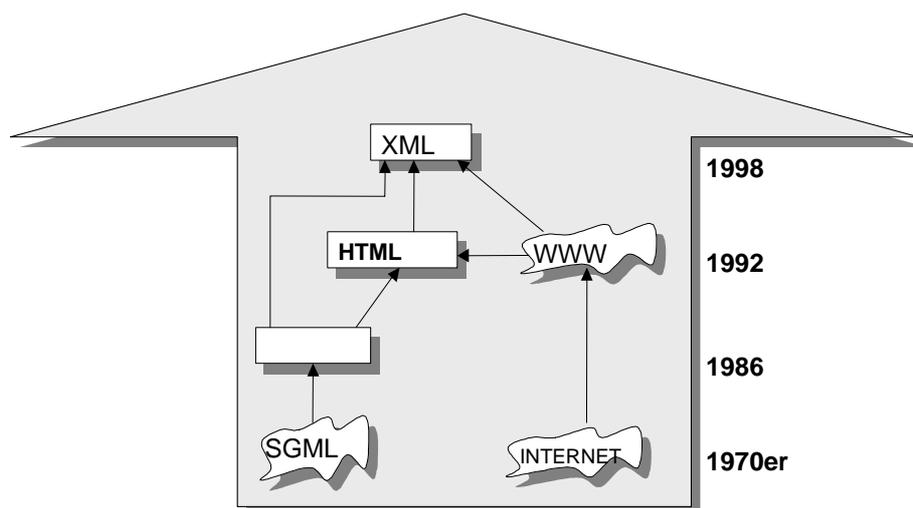


Abb. 34: Entwicklung von SGML, HTML und XML

- Firmen & Organisationen können jetzt Auszeichnungssprachen schaffen, die an die eigenen Bedürfnisse angepaßt sind. Beispiel: Elektronische Verträge (vgl. Abschnitt XXX)
- Der Benutzer hat mit XML-Datenformaten die Möglichkeit, zwischen verschiedenen Sichten auf einen Datenbestand auszuwählen.

Ein XML-Dokument setzt sich zusammen aus Elementen, die ihrerseits Elemente und Attribute enthalten können. Die Syntax eines Dokuments, d.h. in welcher Form Elemente unterschiedlichen Typs verschachtelt und welche Attribute einem Elementtyp zugewiesen werden können, ist in einer sog. Dokumententypdefinition (engl. Document Type Definition, DTD) festgelegt. Die DTD selbst kann Teil des XML-Dokuments sein oder von diesem als DTD referenziert werden. Da eigentlich erst mit Hilfe der DTD die Syntax eines Dokumententyps festgelegt wird, spricht man bei XML auch von einer Metasprache.

Elemente können einen Inhalt besitzen (d.h. untergeordnete Elemente oder Fließtext) und/oder Attribute. Es ist eine Entscheidung des DTD-Designers, ob gewisse Information in Elementen oder in Attributen abgelegt wird. Als Beispiel dienen die folgenden Variationen einer Adressinformation:

```
...
<Adresse>
  <strasse> Schlankreye 61 </strasse>
  <plz> 20144 </plz>
  <ort> Hamburg </ort>
</Adresse>
<nächstes-element> ...
```

und:

```
...
<Adresse strasse="Schlankreye 61" plz="20144" ort="Hamburg">
<nächstes-element> ...
```

Die korrespondierenden DTDs würden folgendermaßen aussehen:

```
<!DOCTYPE adresse [
<!ELEMENT adresse (strasse, plz, ort) >
<!ELEMENT strasse (#PCDATA) >
<!ELEMENT plz (#PCDATA) >
<!ELEMENT ort (#PCDATA) >
]>
```

und:

```
<!DOCTYPE adresse [
<!ELEMENT adresse EMPTY >
<ATTLIST adresse
  id ID #required
  strasse CDATA #required
  plz CDATA #required
  ort CDATA #required >
]>
```

Dabei lassen sich zu den Addressfeldern zusätzliche Metainformationen hinzufügen, wenn sie als Attribute deklariert werden. Das Attribut "id" im zweiten Beispiel ist ein Standardattribut, welches automatisch dem betreffenden Element (hier vom Typ "adresse") eine eindeutige ID zuweist.

Im Gegensatz zu HTML spielt die Formatierung eines Dokuments bei der Ausgabe auf dem Drucker oder dem Bildschirm keine Rolle. Diese Funktion wird in XSL definiert - der Extended Styleset Language - einem weiteren Standard der XML-Familie.

Ein XML-Dokument heißt wohlgeformt, wenn folgende vier Regeln erfüllt werden:

- Alle Elemente, die einen Inhalt haben, müssen sowohl ein Start-Tag als auch ein End-Tag haben.
- Alle Attribut-Werte müssen in Anführungszeichen stehen.
- Jedes leere Element (z.B.) muß entweder mit „</>“, enden, oder man muß einen regulären Ende-Tag einführen (z.B.:).
- Elemente müssen sauber ineinander eingebettet werden.

Einer wohlgeformten XML-Instanz wird keine DTD zugrundegelegt.

Beispiel:

```
<?XML Version = „1.0“ ?>
<gespräch sprache="Deutsch">
  <gruß> Hallo </gruß>
  <antwort> Gleichfalls </antwort>
```

```
</gespräch>
```

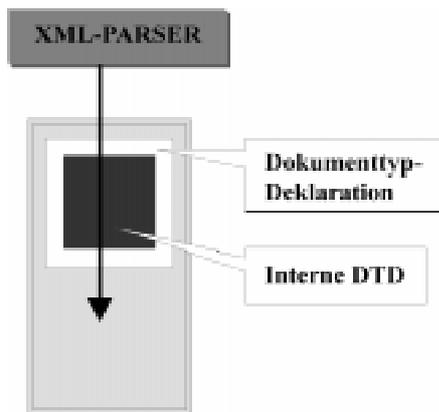
Ein XML-Dokument wird als gültig (engl. valid) bezeichnet, wenn es sich wie ein SGML-Dokument verhält, d.h. wenn das XML-Dokument sich an die in der DTD formulierten Beschränkungen hält.

```
<!ELEMENT gespräch
  (gruß, antwort)>
<!ATTLIST gespräch
  sprache CDATA #IMPLIED>
<!ELEMENT gruß
  (#PCDATA)>
<!ELEMENT gruß
  (#PCDATA)>
```

Beim Zugriff auf ein gültiges XML-Dokument muß für den Parser bekannt sein, wo sich die DTD befindet:

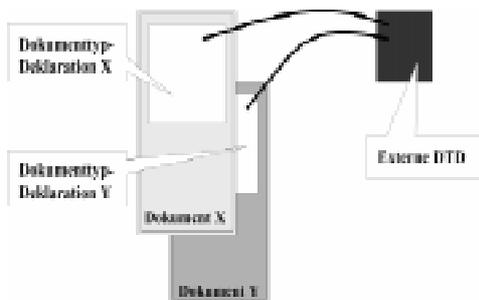
- 1) DTD befindet sich im Dokument selbst.
- 2) DTD ist lokal auf dem Rechner.
- 3) DTD wird vom Netz geladen.
- 4) DTD ist im Browser integriert.

Die DTD steht direkt im Dokument bzw. in der Dokumenttyp-Deklaration.



Die DTD befindet sich als separate Datei außerhalb der XML-Instanz. Eine spezielle Instruktion in der Document Type Deklaration verweist auf die DTD-Datei. Beispiel:

```
<!DOCTYPE gespräch SYSTEM "gespräch.dtd" >
```



Semantische Tags in einem XML-Dokument haben nur Aussagekraft über die Bedeutung der Elemente und nicht wie bei HTML, wo die Tags entweder die Position oder die Formatierung der Elemente beinhalten.

Der XML-Namensraum

DTDs werden vom XML-Dokument aus über eine URI referenziert:

```
<!DOCTYPE adresse SYSTEM "http://www.merz.com/dtds/adresse.dtd">
```

Der Vernetzung von HTML-Dokumenten ähnlich, können DTDs damit beliebig im WWW referenziert werden. Hier könnte es nun passieren, daß zwei Autoren die gleichen Namen für Elemente verwenden. Wenn diese unterschiedlichen DTDs von unserem XML-Prozessor geladen werden, wird er intern eine Liste von Elementtyp-Definitionen verwalten. Sobald aus einer DTD eine Definition für einen Elemente geladen wird, dessen Name bereits eine vorherige DTD verwendet, wird deren Definition überschrieben. Um dies zu verhindern, kann ein XML-Autor verwendete DTDs durch Namenszusätze so qualifizieren, daß Elementnamen eindeutig zugeordnet werden können. Dazu ein Beispiel:

```
<?xml version="1.0"?>
<message xmlns:edi='http://www.ecommerce.com/edi-schema'
         xmlns:vcard='http://www.vcard.org/vcard-schema' >

  <edi:header> ...
    <edi:sender-info>
      <vcard:address-info>
        ...
      </vcard:address-info>
    ...
  </edi:header>
</message>
```

Hierbei werden Elemente, die nach der Syntax des VCARD-Standard (vgl. auch Kap. XXX) organisiert sind, eingebettet in ein Element vom Typ "edi:sender-info", der von einer anderen Organisation festgelegt wurde. Damit ist erkennbar, welche zusätzliche Qualität XML gegenüber HTML bietet: Nicht nur auf der inhaltlichen Ebene können Dokumente vernetzt werden - das gleiche gilt für DTD-Standards selbst! Die Folge ist eine wohl nie dagewesene Entfesselung von "Standardisierungs-Energie", denn zunächst definiert sich jede Anwender-Gemeinde ihre DTDs selbst, ohne auf langfristige Entscheidungen des Web-Consortiums warten zu müssen. Aber auch die Einbeziehung dieser DTDs ist ohne weiteres möglich, da sie dank des festgelegten XML-Namensschemas integriert werden können. Lediglich der Präfix "XML" ist vom Web-Consortium reserviert worden.

In späteren Abschnitten werden wir uns noch mit verschiedenen Anwendungen von XML im Electronic-Commerce-Bereich beschäftigen.

7.1.7 XSL

Bei HTML ist das Leben leicht (aber unflexibel): für jedes Tag ist nicht nur qua Standard festgeschrieben, auf welche Weise der markierte Bereich zu interpretieren ist (Semantik), sondern auch, wie zu visualisieren ist (Präsentation). Ein HTML-Programmierer lernt z.B. nur einmal das Tag <H1> kennen, um Überschriften zu markieren und weiß dabei genau, wie die Überschrift dargestellt wird. Dies gilt im übrigen für alle Web-Browser.

Da nun XML aber über den Bereich des WWW hinausgeht (z.B. XML/EDI), kann es sein, daß mit den unterschiedlichen Anwendungskontexten auch unterschiedliche Visualisierungen einhergehen. Man denke beispielsweise an Redaktionssysteme: Im Unternehmen erstellt ein Redakteur einen Text zur Unternehmenspräsentation. Im Texteditor möchte er sich dabei nicht mit der graphischen Positionierung der Corporate Identity des Unternehmens oder anderen gestalterischen Fragen auseinandersetzen. Er benötigt lediglich die Tags <Abstract>, <Überschrift>, <Kunden>, <Projekte> und <Kontaktinformation>. Eine eigene DTD "Unternehmensdarstellung" wird für das Textdokument verwendet. Der Texteditor unterstützt dabei den Redakteur, indem beispielsweise Kunden, Projekte und die Kontaktinformation als hierarchisch eingerückte Elemente im fließenden Text editiert werden.

Wenn nun dieser Text über den Web-Server veröffentlicht wird, bestehen andere Anforderungen: Kunden, Projekte und Kontaktinformation sind in einen HTML-Frame darzustellen, jeweils mit eigenen Farbtönen unterlegt. Zudem verfügt der Web-Server über eine Komponente, die aus jedem Dokument einen Extrakt entnimmt und diesen in die Datenbasis der lokalen Suchmaschine einträgt. Zu diesem Zweck wird wiederum auf den mit <Abstract> markierten Bereich zugegriffen.

Die Anforderung ist also, das gleiche XML-Dokument in unterschiedlichen Anwendungskontexten unterschiedlich darzustellen. Genau zu diesem Zweck dient die XSL - Extended Stylesheet Language. XSL dient zur Trans-

formation von XML-Dokumenten in andere Syntaxen und anders benannte Strukturierungselemente. Ein Standardanwendung ist dabei die Transformation in HTML; wir werden jedoch noch verschiedene andere Anwendungen von XSL kennenlernen (XXX Ja)?

XSL sollte folgende Designregeln beachten:

- XSL unterstützt unterschiedliche Verarbeitungsmodi wie Browsen, Drucken, interaktives Editieren sowie das Konvertieren von Dokumenten zwischen unterschiedlichen "XML-Dialekten".
- Dabei erlaubt XSL die Rückwärtskompatibilität zum WWW, indem anhand eines Standard-Stylesheets HTML-Dokumente als XML-Dokumente interpretiert und wieder in der HTML-Formatierung ausgegeben werden können.
- XSL kann neben der Formatierung zur Visualisierung auch die Formatierung in Standard-Formate - z.B. das spezieller EDI-Nachrichten, unterstützen.
- XSL ist eine deklarative Sprache. Anhand von Regeln wird festgelegt, welche Elemente eines XML-Dokuments wie zu verarbeiten sind. Dabei wird jedoch kein Programmablauf festgelegt.
- XSL wurde optimiert für die bequeme Formatierung einfacher, häufig auftretender Strukturen. Dabei steht es jedoch offen, beliebig komplexe Regeln zu definieren. XSL unterliegt dabei keinen Algorithmischen Einschränkungen.
- XSL unterstützt flexible Mechanismen zur Erweiterbarkeit, so daß die Integration von Dokumenten und deren Formatierungen flexibel, dezentral und autonom durch unabhängige Teilnehmer im Internet vorangetrieben werden kann.
- XSL spielt dabei mit anderen Web-Standards so zusammen, daß Redundanzen weitgehend vermieden werden konnten. Diese Standards sind im speziellen: XML, XLL, DOM, HTML und ECMA Script.
- Dabei lassen sich XSL-Stylesheets selbst in XML repräsentieren. Entsprechend steht eine standardisierte XSL-DTD zur Verfügung. Dies hilft, bereits auf dem Markt verfügbare Werkzeuge zur Erstellung und Verarbeitung von XSL-Deokumenten einzusetzen.
- XSL-Stylesheets sind einfach strukturiert und damit für den menschlichen Benutzer lesbar.

Ein XSL-Stylesheet besteht dabei aus zwei Komponenten: Einer Sprache zur Transformation von XML-Dokumenten und einem standardisierten Vokabular, mit dem die Formatierung des Dokuments festgelegt wird.

...

Ein XSL-Dokument besitzt immer ein Element *xsl:stylesheet*. Im folgenden ist ein einfaches Beispiel beschrieben, das eine Folge von <Absatz>-Elementen konstruiert, die wiederum <Hervorhebung> enthalten.

Das Attribut *result-ns="fo"* zeigt an, daß ein Baum generiert wird, für den das referenzierte Vokabular verwendet wird. Für das Wurzel-Objekt wird festgelegt, das eine Seitensequenz festgelegt wird mit Serifenfonts. <Absatz>-Elemente transformiert die XSL-Maschine in Elemente des Typs <Block>. Der enthaltene Text wird in 10-Punkt-Schrift mit 12-Punkt Zwischenraum vor dem betreffenden Ansatz dargestellt.

```
<xsl:stylesheet
  xmlns:xsl="http://www.w3.org/TR/WD-xsl"
  xmlns:fo="http://www.w3.org/TR/WD-xsl/FO"
  result-ns="fo">

  <xsl:template match="/">
    <fo:page-sequence font-family="serif">
      <xsl:process-children/>
    </fo:page-sequence>
  </xsl:template>

  <xsl:template match="para">
    <fo:block font-size="10pt" space-before="12pt">
      <xsl:process-children/>
    </fo:block>
  </xsl:template>
</xsl:stylesheet>
```

Das xsl:stylesheet-Element kann weitere Stylesheet-Definitionen enthalten, die mit Hilfe von URIs referenziert

werden, Makros und globale Konstanten definieren und über das WWW geladen werden können. Mit "match" wird der Elementtyp identifiziert, für den die Regel anzuwenden ist. Im Beispiel wurden Formatierungsanweisungen aus dem "fo"-Vokabular verwendet. Da sich die XSL-Regeln auf Knoten einer Hierarchie beziehen, ist noch festzulegen, an welcher Stelle die Verarbeitung der Kind-Elemente fortzusetzen ist. Dies erfolgt durch `<xsl:process-children/>`.

XSL-Templates

Nachdem für ein XML-Element die betreffende Regel identifiziert wurde, instanziiert der XSL-Prozessor die Schablone (engl.: Template) dieser Regel. Sie enthält Textkonstanten, Resultatelemente oder Instruktionen, um Teile des Resultatbaumes zu erzeugen. Instruktionen werden wiederum über das XML-Namensschema referenziert. Sie erlauben beliebige Programmlogik, so daß XSL als algorithmisch vollständige Programmiersprache aufgefaßt werden kann.

```
<xsl:template match="chapter/title">
  <fo:rule-graphic/>
  <fo:block space-before="2pt">
    <xsl:text>Chapter </xsl:text>
    <xsl:number/>
    <xsl:text>: </xsl:text>
    <xsl:process-children/>
  </fo:block>
  <fo:rule-graphic/>
</xsl:template>
```

Beispiel

```
<customers>
  <customer>
    <name>...</name>
    <order>...</order>
    <order>...</order>
  </customer>
  <customer>
    <name>...</name>
    <order>...</order>
    <order>...</order>
  </customer>
</customers>
```

führt zu einer HTML-Tabelle, wenn die folgende XSL-Regel verwendet wird:

```
<xsl:template match="/">
  <HTML>
    <HEAD>
      <TITLE>Customers</TITLE>
    </HEAD>
    <BODY>
      <TABLE>
        <TBODY>
          <xsl:for-each select="customers/customer">
            <TR>
              <TH>
                <xsl:process select="name"/>
              </TH>
              <xsl:for-each select="order">
                <TD>
                  <xsl:process-children/>
                </TD>
              </xsl:for-each>
            </TR>
          </xsl:for-each>
        </TBODY>
      </TABLE>
    </BODY>
  </HTML>
</xsl:template>
```

XSL erlaubt die Kombination mehrerer externer Stylesheets durch Überschreiben, Einschließen oder Einbetten.

- Beim Überschreiben wird ein zuvor existierendes Stylesheet von einem nachträglich definierten über das Tag "xsl:import" importiert. Alle importierten Stylesheets müssen zu Beginn benannt werden. Wurden Regeln unter gleichem Namen in zuvor importierten Stylesheets definiert, werden sie durch die des später importierten überschrieben.
- Beim Einschließen wird das referenzierte XSL-Dokument textuell an der Stelle eingesetzt, an der im übergeordneten Dokument das "xsl:include"-Tag steht. Alle im eingeschlossenen Dokument importierten Elemente überschreiben wiederum die zuvor definierten, wenn ihre Namen übereinstimmen.
- Schließlich kann an beliebiger Stelle in einem XML-Dokument ein Stylesheet definiert werden, das sich nur auf untergeordnete Elemente bezieht. Da XML-Dokumente selbst wieder externe Dokumente referenzieren können, ist die Integration beliebiger autonomer Stylesheets der externen Quellen möglich. Man denke beispielsweise an Nachweise für Lieferquellen eines Produktes, die es den jeweiligen Firmen erlauben, ihre eingebetteten Daten der eigenen Corporate Identity entsprechend zu formatieren. Dies wird im folgenden Beispiel kurz illustriert:

Beispiel:

```
<?xml version="1.0"?>
<?xml:stylesheet type="text/xsl" href="#id(style1)"?>
<!DOCTYPE katalog SYSTEM "katalog.dtd">
  <doc>
    <firmenprofil>
      <xsl:stylesheet xmlns:xsl="http://www.catalog.com/company-
descr-xsl"
                    id="style1">
        <xsl:import href="doc.xsl"/>
        <xsl:template match="id(foo)">
          <fo:block font-weight="bold">
            <xsl:process-children/>
          </fo:block>
        </xsl:template>
      </xsl:stylesheet>
    </firmenprofil>
    <beschreibung>
      <absatz id="foo">
        Dies ist der Text des Absatzes ...
      </absatz>
    </beschreibung>
  </doc>
```

7.1.8 XML/EDI

XXX Bla Bla Bla

	XML/EDI	OO EDI
Schlüsselmerkmale	Einfache Implementierbarkeit Preiswerte Werkzeuge sind verfügbar, um strukturierte, Web-basierte Dokumente zu erstellen und auszutauschen	Einfache standardisierte Implementierbarkeit Vereinfachter Handel auf der Basis von Open-EDI-Szenarien
Infrastruktur	Preiswert und allgemein verfügbar Kommunikationskomponenten sind bereits verfügbar (Internet, Web-Browser und -Server, e-Mail) Werkzeuge zur Nachrichtendefinition (DTD-Editoren) und -verarbeitung (XML-Parser) stehen zur Verfügung Existierende Web-Server/Firewalls erfüllen Sicherheitsanforderungen	Spezialisiert und noch nicht verfügbar Verteilte Objektsysteme als Kommunikationsinfrastruktur für B2B besitzen noch keine Produktreife. CORBA und DCOM sind noch nicht verbreitet. Sicherheitsinfrastruktur durch SSL und Firewalls gegeben.
Industrieunterstützung	Gegeben durch Microsoft, Netscape, Sun sowie alle Anbieter von SGML-Werkzeugen	Es hat sich noch kein Anbieter öffentlich zur OO-EDI-Entwicklung bekannt.
Marktbreite	Sehr groß, XML kann eingesetzt werden für das Dokumentenmanagement, für Autosysteme, für die Informationsrecherche, sowie den Datenaustausch a la EDI.	Beschränkt Nur auf die Kombination von EDI mit Workflow-Management reduziert
Standardisierungsansatz	Mehrere offene Industriestandards (de-facto). XML legt nur das Auszeichnungsformat fest, nicht jedoch das der Nachrichten. Balkanisierung möglich durch Parallelentwicklungen.	Monolithischer De-jure-Standard Alle standardisierten Daten- und Nachrichtenformate müssen von EDIFACT/X12 zentral anerkannt werden.
Entwickler	Diverse Entwickler aus der Internet-Gemeinde.	Noch keine Entwickler, da Standards erst verabschiedet werden müssen
Electronic-Commerce-Produkte	Erste Generation verfügbar Hauptsächlich kleine und mittlere Anbieter sowie Start-Ups: webMethods, InterMax, VEO Systems, Vtopia.	OO-EDI-Standards sind noch nicht vollständig verabschiedet.
Marktanalysen	Gartner Group (im Juli 1998): XML-Unterstützung ist erforderlich für Entwickler von EDI-Produkten ab dem 2. Halbjahr 1999.	Gartner Group geht von einer Marktdurchdringung durch verteilte Objektsysteme wie OO-EDI erst im Jahre 2002 aus.

7.1.9 ICE – Information and Content Exchange

Im Kapitel XXX wurde die Verwaltung von Kunden und ihren Profilen als Kernbestandteil des Virtual Community Management genannt. Die Frage, wie nun Kunden anhand ihrer Profilinformatoren mit sie interessierenden Inhalten versehen werden können, blieb jedoch offen.

Zu diesem Zweck wurde ein weiterer Standard vom Web-Konsortium festgelegt, der helfen soll, Inhalte die zwischen Geschäftspartnern ausgetauscht werden, zu repräsentieren und zu verteilen. Auch hier dient XML als Metasprache zur Festlegung eines entsprechenden Standards, namens ICE (Information and Content Exchange).¹⁴

¹⁴ Informastionen zu ICE finden sich unter: <http://www.w3.org/TR/NOTE-ice>

Das ICE-Protokoll soll Unternehmen helfen, die Inhalte produzieren und diese mit Geschäftspartnern austauschen. In diesem Bereich existiert heute zwar eine Vielzahl Ad-hoc-Lösungen, jedoch besteht das Problem in der schwierigen Übertragbarkeit einer branchen- oder unternehmensspezifischen Lösung auf andere Bereiche.

Inhalteanbieter sind dabei Unternehmen wie Verlage und Nachrichtenagenturen, aber auch Unternehmen, die regelmäßige Geschäftsbeziehungen mit Kunden oder Zulieferern pflegen: als ICE-Inhalte kann man sich also Nachrichten, Wetterkarten, Preislisten, Ausschreibungsinformationen, Bestellungen oder Modekataloge vorstellen.

Da in diesem Bereich der B2B-Commerce besonders vorherrscht, wird mit ICE ein XML-basierendes Protokoll für den Inter-Server-Datenaustausch vorgeschlagen, das einen Rahmen vorgibt, der für vertikale Spezialisierungen branchenspezifisch erweitert werden kann. Dabei kann das ICE-Protokoll mit jeder beliebigen XML-DTD kombiniert werden – Format und Inhalt sind somit unabhängig.

Das Protokoll geht von einer Geschäftsbeziehung zwischen zwei Partnern aus, von denen einer als Anbieter bzw. Verteiler (engl. *Syndicator*) und der andere als Abonnent (*Subscriber*) von Inhalten agiert. Das Protokoll legt damit lediglich Regeln für den Datentransfer fest. Zur Einhaltung dieser Regel wird bei beiden Partnern eine ICE-Software vorausgesetzt, die ICE-Nachrichten zwischen dem internen und dem externen Format konvertiert.

Ein Schlüsselement der Kommunikation ist hier das Request/Response-Modell: Jede Anfrage (Request) erfordert eine Antwort (Response), auch wenn dies nicht immer sinnvoll erscheinen mag. Ein Abonnement beginnt immer mit der Anfrage nach einem Angebotskatalog des Anbieters. Dabei ist die ICE-Software in der Lage, bestimmte Kommunikationsparameter wie z.B. Sicherheits- oder Transportmechanismen zu verhandeln.

Das Protokoll sieht folgende wesentliche Operationen vor:

- *Einrichten eines Abonnements.* Hier werden allgemeine Mechanismen für das Abonnement festgelegt: Beginn- und Endedatum, Zeitpunkte und Frequenzen der Nachrichtenübermittlung, Methode (Push vs. Pull) sowie alternative Lieferadressen. ICE legt dabei auch die Grundlage zur Beschreibung von Metadaten der Lieferung: Copyright-Informationen, Dringlichkeitsstufen etc. Dabei obliegt die Verarbeitung dieser Informationen jedoch der ICE-Anwendung und nicht dem Kommunikationsmechanismus.
- *Datenlieferung.* Inhalte werden in Paketen ausgetauscht. Ähnlich EDI können mehrere Lieferungen in einem Paket übermittelt werden. Ebenso lassen sich inkrementelle Aktualisierungen übertragen. Dabei kann der eigentliche Inhalt in den Datenstrom eingebettet sein oder per URL referenziert werden.
- *Protokollierung (Event Logs).* Da es zu Störungen bei der Lieferung kommen kann, definiert der ICE-Standard ein Format für Log-Dateien, anhand dessen Anbieter und Abonnenten Informationen über ihre Verbindung austauschen können.
- *Sonstiges.* Schließlich unterstützt ICE die Möglichkeit, Nachrichten zu Testzwecken zu generieren oder etwa in Fehlerfällen direkt den Administrator einer ICE-Software zu benachrichtigen.

Von wesentlicher Bedeutung ist natürlich die Abbildung des ICE-Protokolls auf HTTP. Hier wird insbesondere vom HTTP/Post Gebrauch gemacht – der Möglichkeit, größere Datenmengen per "Push" an den Server zu übertragen. Folglich muß der Anbieter über einen Web-Server verfügen, über den die Kommunikation mit seinem internen Softwaresystem erfolgt. Darüber hinaus legt das ICE-Protokoll anhand von XML eine minimale Syntax zur Beschreibung der Protokolldateneinheiten fest:

- *ice-payload* definiert dabei die "Nutzlast" eines ICE-Paketes. Der Inhalt ist nicht unmittelbar in ice-payload eingebettet, zunächst wird noch festgelegt, ob es sich bei der Nachricht um eine Anfrage oder Antwort handelt.
- *ice-request* legt fest, daß es sich um eine Anfrage an den Kommunikationspartner handelt.
- *ice-response* definiert eine Antwort auf eine zuvor erfolgte Anfrage. Evtl. erwartet der Sender dieses Nachrichtentyps eine Bestätigung (Confirmation). Dies wird durch ein XML-Element "Confirmation Required" signalisiert. Anschließend wird vom Anfrager die Übermittlung der entsprechenden Nachricht erwartet, die ihrerseits in ein ice-request eingebettet ist. Da bei ICE jede Anfrage zu beantworten ist, gilt dies auch für die Bestätigung, so daß insgesamt 4 Nachrichten zur Übermittlung eines Datenpaketes ausgetauscht werden können.

Im folgenden ist an einem Beispiel beschrieben, welche ICE-Nachrichten zwischen Anbieter und Abonnent ausgetauscht werden:

Schritt 1: Anfrage nach einem Datenpaket

In diesem Schritt fragt der Abonnent beim Anbieter ein Paket ab:

```
SUBSCRIBER ==> SYNDICATOR:
  HTTP POST:
    <ice-payload>
    <ice-request>
      Get Package
    </ice-request>
  </ice-payload>
```

Schritt 2: Senden des Datenpakets

Anschließend liefert der Anbieter das Paket mit der Anforderung, den Empfang zu bestätigen:

```
SUBSCRIBER <== SYNDICATOR:
  HTTP Response to the POST:
    <ice-payload>
    <ice-response>
      Package: X
      Confirmation Required
    </ice-response>
  </ice-payload>
```

Schritt 3: Bestätigung

Im dritten Schritt bestätigt der Abonnent den Empfang.

```
SUBSCRIBER ==> SYNDICATOR:
  HTTP POST:
    <ice-payload>
    <ice-request>
      Confirmation of Package X
    </ice-request>
  </ice-payload>
```

Schritt 4: "Bestätigung" der Bestätigung

Schließlich erfolgt eine „Bestätigung der Bestätigung“.

```
SUBSCRIBER <== SYNDICATOR:
  HTTP Response to the POST:
    <ice-payload>
    <ice-response>
    </ice-response>
  </ice-payload>
```

Zusätzliche Optionen können verwendet werden, um das ICE-Protokoll weiter zu konfigurieren. Mit Hilfe von *Einschränkungen* (engl.: Constraints) können Inhalte anhand von Ausdrücken auf bestimmte Formate festgelegt werden. Z.B. lassen sich Banner-Bitmaps auf ein vorgegebenes Format prüfen oder Nachrichtentexte auf eine maximale Länge begrenzen. Pakete, die diesem Format nicht entsprechen, werden nicht bearbeitet und eine Fehlermeldung wird generiert. Einschränkungen werden dabei als Referenzen eingebunden.

Die Kommunikation auf der Basis von ICE kann frei kombiniert werden mit Protokollen wie z.B. SSL oder PGP. Zusätzlich besteht die Möglichkeit, in Verbindung mit ICE auch Datenschutzmechanismen zu integrieren, ähnlich denen, die beim P3P festgelegt wurden.

ICE stellt damit einen bedeutenden Schritt zur Automatisierung der Inhaltsverteilung über das Internet dar. Unternehmen wie z.B. Reuters oder Verlage allgemein werden von ICE profitieren, da dank der Integration von ICE-Software in die lokale Web-Server-Umgebung das Abonnieren von Nachrichten, Preisinformationen, Dossiers etc. erheblich einfacher administrierbar wird: Es müssen nämlich nicht mehr die Inhalte selbst administriert werden (z.B. Preislisten), sondern lediglich ihr Datenfluß. "Management" spielt sich damit zunehmend auf der Meta-Ebene ab.

Der ICE-Katalog

In einem ICE-konformen Katalog stellt der Anbieter Angebote für Abonnenten bereit. Dabei ist die Struktur des Katalogs durch eine ICE-Katalog-DTD definiert:

```
<!ELEMENT ice-catalog      (ice-contact, (ice-offer-group | ice-offer)*) >
<!ELEMENT ice-contact      (#PCDATA) >
<!ATTLIST ice-contact
  description      CDATA      #REQUIRED
  lang             CDATA      #IMPLIED
  name             CDATA      #REQUIRED
  sender-id       CDATA      #REQUIRED
  url             CDATA      #IMPLIED
>
<!ELEMENT ice-offer-group  ((ice-offer-group | ice-offer)+) >
<!ATTLIST ice-offer-group
  description      CDATA      #REQUIRED
>
```

Ein Katalog besteht damit aus einer Hierarchie von Angebotsgruppen und Angeboten, die wiederum durch die Angebots-DTD spezifiziert sind:

```
<!ELEMENT ice-offer        (ice-delivery-policy, ice-business-term+) >
<!ATTLIST ice-offer
  constraints-hash      CDATA      #IMPLIED
  constraints-hash-method CDATA      #IMPLIED
  constraints-url       CDATA      #IMPLIED
  description          CDATA      #REQUIRED
  subscription-id      CDATA      #IMPLIED
  atomic-use           (false | true) "false"
  editable             (false | true) "false"
  ip-status            CDATA      #IMPLIED
  rights-holder        CDATA      #IMPLIED
  showcredit          (false | true) "false"
  usage-required       (false | true) "false"
>
```

Das Angebot enthält einen Verweis auf von beiden Parteien akzeptierte Einschränkungen (*constraints-url*). Damit die Konsistenz des Dokuments gewährleistet bleibt, liegt dem Angebot ein Hash-Wert bei, mit dessen Hilfe mögliche nachträgliche Änderungen festgestellt werden können.

- *atomic-use* legt fest, ob der Abonnent den Inhalt im Zusammenhang oder auch in Teilen verwenden darf. Dies kann ein Anbieter beispielsweise für Rabattstaffeln in Verbindung mit Preislisten festlegen. Wie bereits angedeutet, kann jedoch nicht von der ICE-Kommunikationssoftware die Einhaltung dieser Regel erwartet werden. Stattdessen könnte beispielsweise ein Redaktionswerkzeug diese Bedingung anzeigen.
- *editable* legt fest, ob der Inhalt vom Abonnenten modifiziert werden darf.

- *ip-status*: Ein Text, der geistige Eigentumsrechte am Inhalt beschreibt. Auch hier obliegt es der Anwendungssoftware des Abonnenten bzw. den Nutzern, entsprechende Vorkehrungen zur Wahrung dieser Rechte zu treffen. Diese können im einzelnen durch folgende Informationen beschrieben werden:
 - **PUBLIC-DOMAIN**: Es bestehen keine Lizenzrestriktionen bez. des Inhalts.
 - **FREE-WITH-ACK**: Es bestehen keine Lizenzrestriktionen außer der Anforderung, die Quelle des Inhaltes nachzuweisen.
 - **SEE-LICENSE**: Es wird angenommen, daß zuvor ein Lizenzabkommen zwischen Anbieter und Abonnent getroffen wurde. Dies ist ein Hinweis auf das betreffende Dokument. Diese Möglichkeit kann als Standardvariante angenommen werden.
 - **SEVERE-RESTRICTIONS**: Hier greifen besondere zusätzliche Restriktionen, die über etwaige Lizenzvereinbarungen hinausgehen. Eine Anwendungssoftware sollte dies durch eine entsprechende Markierung signalisieren.
 - **CONFIDENTIAL**: Der Inhalt wird als vertraulich deklariert und erfordert besondere Schutzmaßnahmen.
- *rights-holder*: Dieser Text beschreibt den Eigentümer des Rechtes.
- *show-credit*. Wenn dieses Attribut TRUE ist, wird dem Abonnenten explizit signalisiert, daß gegenüber Dritten die Quelle des Inhalts zu nennen ist.
- *usage-required*: Der Abonnent hat dem Anbieter den Verwendungszweck des Inhalts zu nennen, d.h. wer die endgültigen Empfänger der Daten sind. Auch hier legt der ICE-Standard keine Entscheidung über weitere Details zur Realisierung.

ICE-Business-Terms

Ein ICE-Angebot kann neben den vorgenannten Attributen noch weitere Geschäftsbedingungen beider Partner umfassen. Einem Angebot ist dabei eine Liste von Klauseln beigefügt, die jeweils in der folgenden Grammatik definiert sind:

```

<!ELEMENT ice-business-term      (#PCDATA) >
<!ATTLIST ice-business-term
  lang          CDATA          #REQUIRED
  type          (credit | licensing | payment | reporting) #REQUIRED
  url           CDATA          #IMPLIED
>

```

Dabei legt **lang** die verwendete Sprache fest. Alle Klauseln werden in vier Klassen unterschieden (credit, licensing, payment und reporting). Dabei haben diese folgende Bedeutung:

- **Credit**: Weitere Vereinbarungen zur Nennung des Eigentümers bei der Verwendung der Inhalte.
- **Licensing**: Der Text eines evtl. getroffenen Lizenzabkommens.
- **Payment**: Legt die Zahlungsmodalitäten fest für anfallende Lizenzgebühren, die mit der Nutzung der Inhalte entstehen.
- **Reporting**: Beschreibt die vereinbarte Berichtsinformation an den Anbieter – z.B. über die Anzahl der Empfänger der betreffenden Inhalte.

Verhandlung von Abonnements

Zwischen Anbietern und Abonnenten können Angebote erstellt und verhandelt werden. Dabei steht eine Verhandlungssprache mit minimalem "Wortschatz" zur Verfügung. Der Wortschatz besteht aus den "Worten" *Offer*, *Sorry* und *subscription*. Mit *Offer* wird eine vom Sender vertretbare Attributkombination an den Empfänger übermittelt. *Offer* kann jedoch auch als Antwort auf ein vorheriges Angebot erwidert werden. Mit *Sorry* erfolgt eine Ablehnung des Angebots ohne Gegenangebot. Schließlich wird eine Verhandlung erfolgreich beendet, wenn ein Angebot des Abonnenten mit einem Abonnement beantwortet wird. Der minimale Nachrichtenfluß ist damit:

1.SUB ==> SYN : ice-get-catalog

- 2.SUB <== SYN : ice-catalog
- 3.SUB ==> SYN : ice-offer [offer-from-catalog]
- 4.SUB <== SYN : ice-subscription

Falls eine Verhandlungsrunde erforderlich ist, in der beispielsweise der Abonnent das Angebot modifiziert, wird die Konversation etwas komplexer:

- 1.SUB ==> SYN : ice-get-catalog
- 2.SUB <== SYN : ice-catalog
- 3.SUB ==> SYN : ice-offer [offer-from-catalog]
- 4.SUB <== SYN : Error 441, ice-offer [counter-offer]
- 5.SUB ==> SYN : ice-offer [the very same counter-offer from step 4]
- 6.SUB <== SYN : ice-subscription

Zukünftiger Einsatz von ICE?

Für ein Unternehmen, das ICE unterstützt, kann man sich etwa folgenden Geschäftsprozeß vorstellen: Mit einem Kunden wird zunächst ein Vertrag ausgehandelt, der festlegt, unter welchen Umständen das Abonnement der Online-Preisinformation erfolgt. Diese Regelungen schließen Sicherheitsmaßnahmen ein sowie eine Beschreibung der Häufigkeit von Aktualisierungen. Auch das gemeinsame Verständnis hinsichtlich Ausnahmefällen wie ausgefallenen Lieferungen etc. wird festgehalten. Nach Unterzeichnung des Vertrages werden die betreffenden Regeln und Optionen für den neuen Abonnenten festgelegt. Dabei wird ihm Zugang zum Angebots-Katalog verschafft. Metainformationen zum Datenformat der Preisliste (z.B. als DTD) werden dem Abonnenten zur Verfügung gestellt. Anschließend richtet dieser seine ICE-Software so ein, daß das Preislistenformat des Anbieters konvertiert werden kann in sein lokales. Von nun an können die ICE-Operationen einsetzen und die regelmäßige Aktualisierung der Preisliste erfolgen.

ICE kann EDI nicht ersetzen, da es sich nicht um die weitere Strukturierung von „Information and Content“ zu kümmern braucht. Gerade Information und Inhalt ist jedoch der Schwerpunkt, auf den die EDI-Standardisierung abzielt. Damit besteht nur die Hoffnung, das die erhöhte Standardisierungseffizienz von XML hilft, dem Kohärenzproblem, das die Automatisierung des B2B-Commerce mit sich bringt, zu Leibe zu rücken.

Solange dieses Problem nicht in allgemeiner Form lösbar ist, bleibt zunächst nur der Business-to-Business-Consumer-Commerce, bei dem man sich anstelle der vollständigen Software-Integration mit der Kommunikation Software—Benutzer zufrieden gibt.

7.2 Extranets und Broker

Internet- und im besonderen Web-basierte Protokolle lassen sich heute in jeder Netzwerkkumgebung finden. Dies kann unternehmensintern ohne öffentlichen Zugriff sein, dann sprechen wir vom *Intranet*. Allerdings endet das Intranet nicht mit dem LAN des Unternehmens: Wenn die Organisation mehrere Zweigstellen umfaßt oder Mitarbeitern von außen Zugriff gewährt werden muß, damit sie z.B. ihre E-Mail lesen können, so hat die Architektur des Intranets dies zu berücksichtigen. Sie ist also viel mehr an der Organisation des Unternehmens orientiert als an der physikalischen Topologie eines lokalen Netzes.

Von besonderer Bedeutung ist die Absicherung des Intranets durch *Firewalls* gegen externe Angreifer. Das Problem liegt darin, einerseits Mitarbeitern, die sich auf Reisen oder zuhause befinden, Zugang zum Intranet zu gewähren, andere Teilnehmer jedoch nicht über den öffentlichen Bereich hinweg auf interne Informationen durchdringen zu lassen. Smartcard-basierte Authentisierungsverfahren oder Systeme zur Generierung dynamischer Passwörter (vgl. etwa das Produkt SafeWord [XXX]) bieten hier eine Token-basierte Lösung des Sicherheitsproblems.

Das *Internet* ist – wiederum organisatorisch betrachtet – der öffentliche Raum zwischen den Organisationen. Hier greifen keine Verfahrensregeln einzelner Teilnehmer. Jeder kann aktiv z.B. durch einen Web-Server oder passiv durch einen Web-Browser diese Infrastruktur nutzen. Niemand kann dabei jedoch Kontrolle über das Gesamtnetz oder auch nur den logischen Kommunikationskanal zwischen Geschäftspartnern besitzen. Aus diesem Grund sind

beim Intranet für jeden Teilnehmer besondere Schutzmaßnahmen zu ergreifen, um Vertraulichkeit, Integrität, Authentizität und Zurechenbarkeit aufrechtzuerhalten.

Schließlich nimmt das *Extranet* die Rolle eines "kontrollierten" Internet ein: Es gewährt Geschäftspartnern Zugriff auf Daten und Services eines Unternehmens, die gezielt einigen Nutzern zur Verfügung gestellt werden. Dabei können sogar einzelne Personen desselben Partnerunternehmens unterschiedliche Zugriffsrechte besitzen. Das Extranet ist somit beim externen Zugriff auf Unternehmensdaten ähnlich restriktiv wie das Intranet – auch hier muß sich jeder Teilnehmer authentifizieren. Im Kern unterscheidet es sich vom Intranet letztlich wieder nur organisatorisch: während das Intranet nur eigenen Mitarbeitern zugänglich ist, wird das Extranet für Außenstehende eingerichtet. Damit könnte das Extranet auch als *Intranet für kooperierende Unternehmen* definiert werden.

EDI als traditioneller Kommunikationsmechanismus zwischen Geschäftspartnern ist somit ein Vorläufer der Extranet-Anwendungen aus der "Vor-Internet-Zeit" gewesen. Hier hat sich eine mehr oder weniger reife Technologie etabliert, mit deren Hilfe die Integrationen der unterschiedlichen Unternehmens-IT vorangetrieben wurde. Daher liegt heute erhebliches Potential in der Integration des elektronischen Datenaustausches mit Extranets als Kommunikationsgrundlage.

Der geschäftliche Einsatz von Inter-, Intra- und Extranets läßt sich am besten anhand einiger Beispiele verdeutlichen:

- Im *Intranet* werden interne Informationen und Dienste wie etwa Terminkalender, Adressdatenbanken, Raumbelegungspläne, Mitarbeiterinformationen, Projektinformationen oder auch technische Informationen verwaltet. Als Dienste stehen zudem die üblichen Internetdienste wie E-Mail, WWW, Telnet und FTP zur Verfügung. Auch hier besteht der zusätzliche Nutzen des Intranets in der Verwendung von Web-Technologien bei der Aufbereitung, Archivierung und Unterstützung der Volltextsuche nach internen Daten. Beim Intranet haben grundsätzlich alle Mitarbeiter Zugang zum Netz und zu einigen allgemeinen Diensten. Jedoch ist es üblich, daß einzelne Abteilungen Dienste anbieten, für die nicht jeder Mitarbeiter autorisiert ist.
- Beim *Internet* stehen Informationen für anonyme Besucher der Web-Site im Vordergrund: Marketing-Informationen, Produktinformationen, Preislisten, Ankündigungen, Dienste zur Unterstützung von Online-Communities (Maillisten, Chat-Gruppen etc.). Üblicherweise wird für anonyme Besucher meistens eine Möglichkeit vorgesehen, sich zu identifizieren, um beispielsweise gezielte Werbeinformation zuzusenden oder um eine Online-Bestellung durchzuführen. Diese Teilnehmer treten spontan in Erscheinung und sind meistens Privatpersonen.
- Das *Extranet* dient der engeren Kopplung kooperierender Unternehmen. Entlang der Wertschöpfungskette eines Unternehmens sind es vor allem Vertriebspartner und Zulieferer, die Extranet-Teilnehmer sind. Vertriebspartner erhalten Zugriff auf interne Produktinformationen, Ankündigungen, Marktanalysen und andere Marketinginformation. Zulieferer werden in die Lage versetzt, an Ausschreibungsverfahren teilzunehmen, Angebote einzureichen oder durch einen Zugriff auf Funktionen der internen Geschäftsanwendung Einkaufspreise des Kunden zu aktualisieren. Extranet-Teilnehmer treten nicht spontan in Erscheinung, sondern sind wohlbekannt und in ihrer Anzahl je nach Komplexität eines Unternehmens stark begrenzt. Ähnlich einem Intranet werden Extranet-Teilnehmer hinsichtlich ihrer Zugangsberechtigung individuell verwaltet. Kunden wird der Zugang zum Extranet gewährt, um einen individuellen Support in Anspruch nehmen zu können oder um Dienste im Rahmen der Kundenbetreuung zu nutzen. Auch unterstützende Dienstleister wie Banken, Steuerberater oder auch das Finanzamt könnte ein Extranet installieren, um Kunden, Klienten oder Steuerzahlern Dienste für den Datenträgeraustausch, Homebanking oder zur Ermittlung der Konditionen zur Kreditvergabe für die Einreichung von Buchungsdaten oder für die Steuererklärung bereitzustellen.

In jeder dieser Extranet-Anwendungen wird der Geschäftspartner individuell verwaltet und besitzt individuelle Zugriffsrechte. Wächst die Anzahl der verwalteten Partner, nehmen damit (meistens) die Varianten der Zugangsberechtigung sowie die Komplexität ihrer Verwaltungsdaten ab. Am anderen Ende dieser Skala befinden wir uns wieder in der Situation "Online-Shop im Internet": Viele Kunden (vorwiegend Privatpersonen) besitzen die gleiche Zugangsberechtigung (entweder keine oder eine allgemeine z.B. zur Aktualisierung des Produktes) und ihre Verwaltungsdaten sind homogen (Transaktionsdaten). Folgende Tabelle faßt die bisherigen Feststellungen zusammen:

Tabelle XXX: Internet – Intranet – Extranet

Zugang zum Unternehmen über	Internet	Intranet	Extranet
Vorwiegende Nutzung durch:	Anonyme Öffentlichkeit	Mitarbeiter	Geschäftspartner, Kunden, Lieferanten
Sicherheitsmaßnahmen	Schutz vor Manipulation, Authentisierung, Zurechenbarkeit	Zugangsschutz durch Firewall, Autorisierung für Nutzung von Diensten	Zugangsschutz durch Firewall, Autorisierung für Nutzung von Diensten, Authentisierung, Zurechenbarkeit
Benutzergruppen	Keine bis wenige	Viele	Viele
Unterstützung von Online-Communities	Maillisten, Mail-Archive, Chat zwischen Kunden	Maillisten	Maillisten, Mail-Archive
Daten	Marketing-Information, Produktinformationen	Mitarbeiterlisten, Dokumentenrepository, Verwaltungsdaten	Marktinformationen, Ausschreibungen, Preislisten, Produkt- und Vertriebsinformationen, EDI

Sein Extranet wird von jedem Unternehmen selbst verwaltet, es ist quasi ein Vorgarten mit Wächter an der Gartenpforte und einem weiteren Wächter am Hauseingang. Vor der Gartenpforte befindet sich das Internet und im Hause das Intranet:

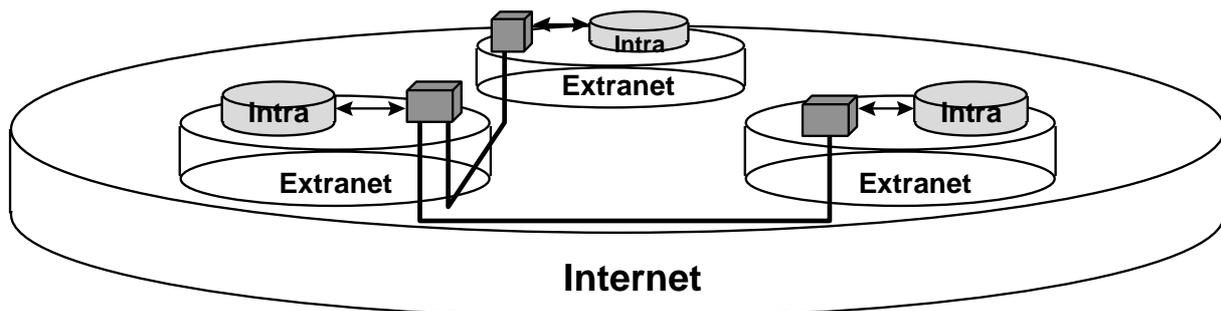


Abb. 35: Internet, Intranet und Extranet

Stand und Entwicklung der Extranet-Nutzung

In vielen Unternehmen werden zur Zeit Extranets eingerichtet. Man geht davon aus, daß im Jahr 2000 bereits die Hälfte aller Unternehmen über Extranets miteinander verbunden sind [XXX Lufthansa AirPlus Servicekarten GmbH, Studie: "Vernetzung zum Wettbewerbsvorteil machen: Electronic Commerce im Business-to-Business-Bereich"]. Nach Auffassung der Autoren werden Extranets EDI-Systeme in Zukunft vom Markt verdrängen: Im Jahre 2001 werden rund 40 Prozent und 2002 etwa 70% des elektronischen Geschäftsverkehrs über Extranets abgewickelt werden. Dies entspricht in Europa ca. 250.000 Unternehmen.

- 35 Prozent der Unternehmen erhoffen sich laut AirPlus-Studie durch den Einsatz von Web-EDI vor allem Kosteneinsparungen durch effizientere Betriebsabläufe.
- 32 Prozent wollen dadurch den Kundenservice verbessern, und
- 18 Prozent den Umsatz steigern.

Die Studie sieht in der mangelnden Kompatibilität der Netzinfrastrukturen eine der Haupthürden. Eine Lösung besteht im Outsourcing des Web-Server-Betriebs an ISPs, die einen solchen Betrieb als Service anbieten. 40 Prozent aller Unternehmen bevorzugen eine solche Lösung, im Jahre 2000 werden dies sogar über 90% sein. Die Rolle des Extranet-Betreibers wird dabei ebenfalls erweitert: Er tritt als Elektronischer Notar auf, der aus einer neutralen Position heraus Geschäftstransaktionen protokollieren kann. Nach der AirPlus-Studie liegt nämlich eine weitere Hürde beim B2B-Commerce in der mangelnden Beweisbarkeit von Transaktionen.

Folglich ist zu erwarten, daß im Laufe der Zeit Extranet-Dienstleistungen zunehmen von neutralen Providern

angeboten werden.

7.2.1 Beispiele für Intranet- und Extranet-Anwendungen

7.2.1.1 Auktionen

Die Auktion ist ein Verfahren, mit dessen Hilfe eine Ressourcenallokation – also die Zuordnung von Geld und Gütern zwischen Anbietern und Nachfragern – effizient durchgeführt werden kann. Ganze Marktplattformen, bei denen eine beliebig hohe Anzahl Nachfragern einer ebenso beliebigen Anzahl Anbietern gegenüberstehen, lassen sich durch Auktionssysteme effizient betreiben.

Auktionen lassen sich überall einsetzen, wo ein marktwirtschaftlicher Koordinationsprozess erforderlich ist. Dies gilt sogar auch für innerbetriebliche Koordinationsaufgaben: Abgesehen von einem prohibitiven Kostengefüge, könnte durchaus eine Fertigungsstufe bei der Automobilherstellung ihre erforderlichen Ressourcen (Mitarbeiter, Strom, Material) für jedes einzelne Fahrzeug anhand einer Auktion beschaffen. Nun ist die "klassische" Auktion, bei der eine physische Präsenz von Bietern und Anbietern erforderlich ist, als Koordinationsmechanismus zu teuer. Sie rechnet sich erst bei einem gewissen Mindestpreis und vor allem auch dadurch, daß ein signifikanter Anteil des Transaktionsvolumens als Provision an den Auktionator abzuführen ist.

Internet-Auktionen sind hingegen preiswert in ihren Betriebskosten: Sie sind eine Extranet-Anwendung, bei der davon ausgegangen werden kann, daß die Bieter dem System bekannt sind und eine entsprechende Sicherheitsinfrastruktur zur Verfügung steht. Das Auktionssystem greift also auf die existierende Extranet-Infrastruktur zurück. Damit reduzieren sich die Hauptkomponenten des Systems auf folgende Komponenten:

- *Angebotsdatenbank.* Hier stellt ein Unternehmen das angebotene oder nachgefragte Produkt einschließlich seiner Spezifikation ein.
- *Bieterverwaltung.* Dieses System greift auf die Verwaltungsfunktionen des Extranet zurück, um Bieter und deren Angebote zu verwalten.
- *Transaktionsverwaltung.* Nach dem Zuschlag an einen Bieter sind die Transaktionsdaten (Angebot, Bieter, Gebot) festzuhalten und die Transaktion abzuwickeln.
- *Auktionsprozeß.* Diese Software legt Auktionstermin und -form fest, leitet den Prozeß der Verhandlung ein und wickelt diese ab, indem über mehrere Iterationsstufen das beste Gebot herausgefiltert wird.

Lufthansa's InfoFlyway

Ein bekanntes und allgemein zugängliches Beispiel ist der Info-Flyway der Lufthansa (www.XXX.de). Hier werden vorgegebene Flüge versteigert. In seiner Pilotphase war dieser Dienst für alle Internet-Teilnehmer zugänglich, heute muß man sich als Bieter mit seiner Miles-and-More-Nummer registrieren. Diese Maßnahme hat zwei Gründe: zum einen fördert sie die Kundenbindung durch Erwerb einer "Member-Karte", zum anderen vereinfacht sie den Abrechnungsprozeß: es ist nicht der beschwerliche Weg einer Payment-Gateway-Anbindung wie im Bereich des Consumer-oriented Commerce erforderlich. Statt dessen kann die Rechnungslegung über die bereits bestehende Finanzbuchhaltung erfolgen.

7.2.1.2 Ausschreibungssysteme

Großunternehmen und die öffentliche Verwaltung vergeben Aufträge von einem Mindestvolumen an in Form einer öffentlichen Ausschreibung (Behörden sind sogar dazu verpflichtet). Dabei ist die Prozedur einfach: In einem öffentlichen Journal wird die Ausschreibungsinformation publiziert. Diese umfaßt eine erste Spezifikation der zu liefernden Produkte oder Dienstleistungen sowie weitere Informationen wie Fristen, Randbedingungen und eine Adresse, von der die vollständige Spezifikation abgerufen werden kann.

Gebote werden zwischen der Veröffentlichung und dem Ablauf der Frist eingereicht. Die Entscheidung über den Zuschlag erfolgt anhand der Ausschreibungskriterien. Dies muß nicht notwendigerweise das Angebot mit dem niedrigsten Preis sein, da seine Qualität von einer Vielzahl Faktoren abhängt. So kann ein Angebot mit 5-jähriger 24-Stunden-Gewährleistung sich gegenüber einem wesentlich preiswerteren durchsetzen, wenn es im Interesse des Auftraggebers liegt, einen kontinuierlichen Betrieb aufrechtzuerhalten.

Der wesentliche Unterschied zwischen Auktions- und Ausschreibungssystemen liegt folglich in der Komplexität der Produktspezifikation. Bei Auktionen kann evtl. die Spezifikation des Objektes komplex sein (z.B. eine Eigentumswohnung), die des Gebotes ist auf jeden Fall einfach – sie besteht lediglich im Preis. Bei der Ausschrei-

bung sind üblicherweise Objekt *und* Angebot komplex, daher versagt hier eine automatische Unterstützung zur Ermittlung des besten Bieters.

Ausschreibungsverfahren bei der Forschungsförderung

Ein öffentliches Ausschreibungsverfahren wird beispielsweise bei der EU-Kommission in Brüssel eingesetzt, um Projektkonsortien die Möglichkeit zu geben, Mittel zur Forschungsförderung einzuwerben. Im Rahmen des Fünften Rahmenprogrammes wird Konsortien die Möglichkeit geboten, Mit Hilfe einer Software die wesentlichen Angebotsdaten zu erfassen und an die EU-Kommission zu senden. Jeder Bieter besitzt dabei einen individuellen Schlüssel, der zur Verschlüsselung und Authentisierung des Projektvorschlags eingesetzt wird. Nach Eingang wird der Konsortialführer per Fax über den Zugang der Daten benachrichtigt. Dieser Mechanismus mußte heute noch auf klassische Dienste wie Fax zurückgreifen, noch nicht für alle Bewerber die Möglichkeit zur Authentisierung mit Hilfe von Signaturschlüsseln besteht. Für die Zukunft ist jedoch geplant, auch das Signieren mit elektronischen Unterschriften zulassen, so daß eine vollständige Abwicklung über das Internet realisierbar wird. Zu diesem Zweck wird eigens eine Zertifizierungsautorität für Bewerber eingerichtet. Auf lange Sicht läßt sich dann das gesamte Verfahren einschließlich der Einbindung externer Gutachter vollständig automatisieren.

Review-System für wissenschaftliche Konferenzen

Ein weiteres Beispiel einer Extranet-Anwendung ist ein Verfahren, welches wir an der Universität Hamburg im Jahre 1998 zur Verwaltung und Begutachtung eingereicherter Forschungsbeiträge für unsere Konferenz TREC'98¹⁵ eingesetzt hatten. Mit einer gewissen Abstraktion läßt sich bei der folgenden Beschreibung leicht erkennen, wie ein solches System auch für kommerzielle Einsatzbereiche genutzt werden kann.

Grundsätzlich erfolgt die Ausschreibung zur Einreichung von Forschungsbeiträgen für wissenschaftliche Konferenzen in folgenden Schritten:

1. *Bekanntgabe der Konferenz.* Innerhalb der Fachgemeinschaft wird ein sogenannter *Call-For-Paper* veröffentlicht, der Schwerpunktthemen, Umfang und Fristen zur Einreichung von Beiträgen enthält. Im Internet werden dazu News-Gruppen, Maillisten und Uploads auf einschlägigen Web-Servern verwendet, um eine möglichst große Adressatenzahl zu erreichen.
2. *Einreichung der wissenschaftlichen Beiträge.* Zu diesem Zweck wird über den Web-Server des Programmvorsitzenden ein anonymer Benutzerzugang eingerichtet, der es Autoren ermöglicht, per FTP oder E-Mail Beiträge einzureichen. Web-Formulare, in die Autoren Adressinformationen eintragen, helfen, die Beiträge automatisch zu verwalten.
3. *Weiterleitung der Beiträge zur Begutachtung durch Mitglieder des Programmkomitees.* Die Gesamtzahl der Beiträge wird nun gleichmäßig auf die Mitglieder des Programmkomitees verteilt. Dabei muß jeder Beitrag mindestens von einer festzulegenden Anzahl an Gutachtern beurteilt werden. Gutachter sind dem Programmvorsitzenden wohlbekannt und verändern sich nicht in ihrer Anzahl oder Identität. Sie werden daher als "Geschäftspartner" im Sinne des Extranet betrachtet und erhalten damit ein eigenes Passwort für den Web-Server.
4. *Einreichung der Gutachten an den Programmvorsitzenden.* Ein Gutachter authentisiert sich beim Web-Server des Programmvorsitzenden, um seinen Beitrag einzureichen. Dies erfolgt ebenfalls über Web-Formulare, so daß diese Information direkt in die Datenbank eingetragen werden kann. Ein Gutachter kann zwar sein eigenes Gutachten nachträglich einsehen und revidieren, jedoch keines der anderen. Nach Ablauf einer Einreichungsfrist besteht für alle Gutachter die Möglichkeit, zusätzlich auch die Gutachten der anderen zusammen mit den Beiträgen einzusehen. Eine Statistikfunktion liefert dazu ein erstes Ranking.
5. *Review-Sitzung.* Die Teilnehmer der Review-Sitzung entscheiden über das endgültige Ranking der Beiträge sowie über die sachliche und chronologische Aufteilung der Beiträge für das endgültige Konferenzprogramm. Normalerweise erfolgte die Review-Sitzung bisher in Form eines Treffens der beteiligten Personen. Mit Hilfe eines Web-Servers besteht jedoch die Möglichkeit, nicht anwesende Teilnehmer so einzubinden, daß dieses Treffen eher "virtuellen" Charakter annimmt. In Zukunft sollte eine qualitativ verbesserte Multimedia-Integration sogar ein Online-Reviewing in Form von Echtzeit-Diskussionen erlauben. Während der Review-Sitzung werden die erforderlichen Daten über Akzeptanz oder Ablehnung eines Beitrags eingetragen.

¹⁵ Trends in Electronic Commerce, siehe auch <http://vsys-www.informatik.uni-hamburg.de/trec98>

6. *Bekanntgabe des Review-Ergebnisses an die Autoren.* Dieser Schritt erfordert lediglich das Formulieren von Anschreiben für die akzeptierten und abgelehnten Beiträge. Die Benachrichtigung erfolgt vollständig "per Knopfdruck".

Das hier beschriebene Verfahren ist eine typische Extranet-Anwendung, welche es Zulieferern ermöglicht, Gebote über das Internet einzureichen, Externen Beratern Zugang auf die für sie bereitgestellten Ressourcen verschafft und für Intranet-Anwendern eine entsprechende Autorisierungsstufe zur Verwaltung des Ausschreibungssystems bietet.

7.2.2 Das Extranet auf neutralem Boden oder die neuen Mittler

Vergleicht man die Extranets unterschiedlicher Unternehmen, stellt man fest, daß sich viele Anwendungen eher nur im Bereich einiger Varianten und Regeln unterscheiden. Für ein kleines Unternehmen ist jedoch der Betrieb eines eigenen Extranets nicht immer rentabel: Neben den Betriebskosten des Web-Servers und dem Internetzugang sind die Kosten der Softwareentwicklung und die Betreuung des Systems häufig prohibitiv.

Damit ist folglich der Bedarf für einen Markt skizziert, der als Erweiterung der Dienstleistung eines Internet Service Providers aufgefaßt werden kann. Ein solcher *Extranet Service Provider* (ESP) steht kleinen Unternehmen als Plattform für den Betrieb eines Extranets zur Verfügung. Ähnlich einem Mall-Betreiber, stellt der ESP Basisfunktionen wie Kataloge, Auktionssystem, Beschaffungs- und Ausschreibungssysteme zur Verfügung. Ein kleines Unternehmen kann auswählen, welche dieser Systeme benutzt werden sollen und eine Verbindung zu diesem Provider – z.B. per E-Mail – herstellen.

Die größte Gefahr besteht bei einem solchen System in der Ablehnung durch den Kunden, weil er nicht in die Sicherheitsinfrastruktur vertraut. Extranet-Daten sollen schließlich nur einem begrenzten Kreis von vertrauenswürdigen Partnern zugänglich gemacht werden; somit wäre es ein schlechtes Geschäftsmodell, wenn dem ESP-Betreiber selbst Tür und Tor für den Zugriff auf diese Daten geöffnet würden.

Zur Lösung dieses Vertrauensproblems bestehen vielfältige Möglichkeiten: entweder muß der ESP dem Kunden durch den Ruf seiner Organisation das Vertrauen vermitteln, daß seine Daten nicht mißbraucht werden oder es läßt sich anhand einer verifizierbaren Sicherheitsinfrastruktur beweisen, daß der ESP gar nicht erst Einblick oder Manipulationsmöglichkeiten besitzt. Die erste Variante ist jedoch realistischer: VAN-Provider, die den Transfer von EDI-Nachrichten leisten, sind heute genauso in der Lage, unverschlüsselte Nachrichten mitzulesen, wie Telekommunikationsunternehmen beispielsweise Fax-Nachrichten abhören können. Vertraut man diesen Providern, sollte dies auch der Fall sein, wenn sie ESP-Dienste anbieten.

Sicherheitsmechanismen können hingegen die Funktionalität der ESP-Dienste elementar beeinträchtigen: Eine Auktion kann beispielsweise nicht durch den ESP-Provider durchgeführt werden, wenn Spezifikationen und Gebote verschlüsselt eingereicht werden.

7.2.2.1 Beschaffungssysteme

Wer jemals im öffentlichen Dienst tätig war, weiß ein Lied vom Mißverhältnis zwischen Beschaffungsvolumen und -aufwand zu singen: Der berühmte Bleistift für 10 Euro-Cent verursacht mindestens das Hundertfache, wenn er über eine Mittelbedarfsanforderung beschafft werden muß. Aber auch Kleinteile im Wert von bis zu 100 Euro erfordern immer noch einen viel zu hohen Beschaffungsaufwand. Hinzu kommen Kosten, die aus der unkoordinierten Beschaffung in größeren Verwaltungsstrukturen entstehen. Mangels IT-Infrastruktur und einfacher Benutzungsschnittstellen war es bisher nicht möglich, das Beschaffungsvolumen eines Großunternehmens so zu zentralisieren, daß es sich lohnt, mit Hilfe von Ausschreibungssystemen oder einfach nur über Volumenrabatte Kostenreduktionen vorzunehmen. Das Einkaufsvolumen der Deutschen Bank beträgt beispielsweise jährlich mehrere Milliarden Euro. Allein durch die Bündelung von Beschaffungsaufträgen ließen sich bereits Einsparungen im Bereich einiger Millionen realisieren.

Kleinere und mittlere Unternehmen waren bisher nicht in der Lage, durch Bündelung signifikante Kostenreduktionen zu erzielen. Broker können hier jedoch ein Ausweg sein: Wenn der Broker die Rolle der zentralen Beschaffung des Großunternehmens spielt und eine ausreichende Anzahl Unternehmen sich einem solchen Beschaffungsverbund anschließen, sind die gleichen Kostenreduktionen zu erwarten. Voraussetzung ist hier, daß die Beschaffungskosten der Broker-Lösung vergleichbar sind mit der zentralisierten Variante.

Die Funktion des *Beschaffungsbrokers* ist die Verwaltung eines Katalogs, in den angeschlossene Unternehmen ihre Bedarfsmeldungen einspeisen. Ein solches Beschaffungssystem erlaubt es beispielsweise Kliniken oder Zahnärzten, medizinische Großgeräte gemeinsam einzukaufen. Ebenso könnten sich mehrere Handwerksbetriebe, die an unterschiedlichen Orten tätig sind, zusammenschließen, um gemeinsam einen Vertrag mit einem ISP zu

schließen, der unter einer "Corporate Identity" – und dennoch für jeden recht preiswert – einen Internet-Auftritt realisiert.

Letztlich kann sich die Beschaffungsoptimierung bis in den Konsumentenbereich fortsetzen. Warum sollen sich nicht Privatpersonen zusammenschließen können, um bessere Einkaufskonditionen zu erschließen? Heute ist noch nicht zu erkennen, bei welchem Volumen ein Automobilhersteller weich wird: Müssen sich zehn Käufer zusammenschließen, um direkt in Wolfsburg "vom Fließband" einzukaufen oder müssen es 100 sein? Technisch steht die erforderliche Infrastruktur mit dem Internet bereits heute zur Verfügung, was fehlt, ist noch die erforderliche kommerzielle Organisation und Kultur. Für den Hersteller ist es noch ein zu großes Wagnis, diesen Vertriebsweg einzuschlagen – er würde sich sehr viel Ärger mit dem klassischen Händler- und Vertriebsnetz einhandeln.

Dennoch stellt ein solcher Kontingentvertrieb von Autos eine typische Extranet-Anwendung dar: Für das neue VW-Golf-Modell wird folgender Vorschlag veröffentlicht:

<i>"Motorisierung:</i>	<i>100 PS,</i>
<i>Farbe:</i>	<i>Schwarz,</i>
<i>Ausstattung:</i>	<i>"Classic Line",</i>
<i>Fertigstellung der Produktion:</i>	<i>01.12.1999,</i>
<i>Ablauf der Registrierungsfrist:</i>	<i>01.01.1999,</i>
<i>Mindestanzahl Käufer:</i>	<i>1000,</i>
<i>Rabatt:</i>	<i>20%</i>
<i>Abholung:</i>	<i>Fließband C-5, Wolfsburg,</i>
<i><Informationen zur Fertigung von Varianten>,</i>	
<i><Kleingedrucktes>"</i>	

Zu verwalten ist hier eine entsprechend große Anzahl "Geschäftspartner". Die Extranet-Anwendung könnte zudem auch umgekehrt funktionieren: Einkäufern wird die Möglichkeit geboten, Angebote zum Einkauf eines Kontingents einzureichen. Dies würde genauso aussehen wie das oben skizzierte Angebot des Herstellers, nur aus "umgekehrter Richtung". Ein Preisagent könnte dabei die Rolle des Einkaufskoordinators übernehmen und das Käuferkonsortium bei seiner Formierung moderieren.

Eine entsprechende Broker-Anwendung kann mit Phantasie in allen Bereichen des privaten oder geschäftlichen Handels eingeführt werden: Nachbarn organisieren sich für den Einkauf von Rotwein direkt beim Abfüller in Bordeaux, Werften organisieren den Einkauf von Hafenkranen oder das Chartern von Flug- und Hotelkontingenten wird direkt vom Kegelclub organisiert.

Organisatorische Änderungen

Im Bereich der Beschaffungskoordination liegt noch erhebliches organisatorisches Potential brach, das erst in den kommenden Jahren Schritt für Schritt genutzt werden wird. Wie bereits angedeutet, erscheint die klassische Vertriebsstruktur dabei zunächst als Verlierer. Dennoch bedeutet dies nicht, daß diese Unternehmen in Zukunft nicht mehr existieren werden – es ändert sich lediglich ihre Rolle, d.h. ihre Einbindung in das Gefüge der Wertschöpfung. Auch wenn das Auto mit einem Rabatt von 20% direkt an den Kunden verkauft wird, sind hin und wieder Besuche in der Werkstatt erforderlich. Auch für Probefahrten ist der Händler unumgänglich, ein Hersteller kann es sich folglich nicht leisten, diese geographische Nähe zum Kunden zu verlieren. Der höhere Rabatt kann folglich nur eine höhere Planungssicherheit ausgleichen.

Zusammenfassung

Stichworte wie Commoditization, Disintermediation und Reintermediation aus Kapitel XXX werden immer wieder durch die genannten Beispiele widergespiegelt. Dem Extranet kommt dabei eine zentrale Bedeutung als logischer Standort solcher Prozesse zu – unabhängig davon, ob es von einem der Geschäftspartner oder einem neutralen Dritten betrieben wird. Was jedoch auch das Extranet nicht lösen kann die gesamte Automatisierung jenseits der Interoperabilitätsebene – also semantische Kohärenz von Softwarekomponenten, Workflow-Steuerung und andere ökonomisch-juristische Probleme.

7.2.2.2 Broker

Eine etwas andere Funktion als das Beschaffungssystem nimmt der *Broker* wahr. Das Beschaffungssystem dient eher einseitig auf der Käuferseite dazu, die Transaktionskosten des Einkaufs zu reduzieren. Die Frage, welcher Anbieter dabei der günstigste ist, bleibt dabei jedoch offen – im Zweifel ist der Verkäufer bereits bekannt. Wenn dies jedoch nicht der Fall ist, tritt der Broker in Erscheinung und hilft, Anbieter und Nachfrager so zu vermitteln, daß Produktspezifikationen für beide Seiten erfüllt werden.

Nach der Transaktionsphasen-Klassifikation ist der Broker also beim Übergang von der Informationsphase in die Verhandlungsphase zu lokalisieren. Er sorgt für ein gegenseitiges Bekanntwerden "passender" Transaktionspartner. Da der Broker ebenfalls über Angebots- oder Produktspezifikationen der Marktteilnehmer verfügen muß, um eine Vermittlung durchzuführen, agiert er als *zweiseitiges* Ausschreibungssystem: Der Nachfrager spezifiziert das gewünschte Produkt und evtl. einen Preis, den er zu zahlen bereit ist. Gleiches gilt für den Anbieter. Die Bedeutung von Rollen wie "Anbieter" und "Nachfrager" verwischen dabei, da der Preis nur noch als ein Attribut von vielen verstanden wird. Damit dient der Broker in seiner abstraktesten Form als Vermittler von Teilnehmern. Er könnte also auch Tennispartner oder Reisebegleitungen vermitteln. Sein Einsatz im kommerziellen Bereich ist nur eine von vielen Ausprägungen.

Im folgenden wird daher von einem neutralen Broker ausgegangen, der keinem Marktteilnehmer zugeordnet ist. Ein solcher Broker bietet jedem Teilnehmer eine Ausschreibungsschnittstelle, über die Produktspezifikationen veröffentlicht werden können. Im Gegensatz zum Ausschreibungssystem wird keine festgelegte Gemeinschaft von Geschäftspartnern benachrichtigt, sondern nur eine Funktion des Brokers selbst, die prüft, ob ein passendes Gegenangebot existiert. Ist dies der Fall, kommt es zum "Match" und zwischen den beiden Teilnehmern wird eine Verbindung hergestellt. Im anderen Fall kann der Broker die Spezifikation vormerken und bei weiteren Registrierungen anwenden. Sobald eine Spezifikation eingetragen wird, die kompatibel ist, wird schließlich die Verbindung hergestellt.

Mehrparteien-Broker

Interessante Varianten sind Mehrparteien-Broker (siehe dazu die Berichte des COSMOS-Projekts [COSMOS99]). Hierbei werden Spezifikationen für mehrere Dienstleistungen oder Produkte registriert, die als Kombination zu liefern sind. Im Beispiel des virtuellen Unternehmen (Kapitel XXX) würde der Publikationsagent einen solchen Mehrparteien-Broker benutzen, um für die definierten Rollen "Titelbild-Design", "Korrekturlesen", "Anzeigenkampagne" etc. die erforderlichen Instanzen einzusetzen. Bei komplexen Spezifikationen wie etwa dem Publikationsagenten kann der Broker nur eine erste Verbindung auf der Basis einer groben Spezifikation herstellen. Diese Spezifikation könnte beispielsweise nur die Rolle vorsehen, in der sich ein Teilnehmer registriert. Jede weitere Verfeinerung der Spezifikation sollte sinnvollerweise im Anschluß, d.h. im Rahmen der Verhandlungsphase, durch die Teilnehmer selbst vorgenommen werden.

7.2.2.3 Der Trader

Als technologische Grundlage des Brokerage-Prozesses dient ein Dienst, der im Rahmen der ODP-Standardisierung bereits Ende der 80er Jahre als *Trader* diskutiert wurde [XXX]. Nachträglich übernahm auch die OMG im Rahmen der Erweiterung von CORBA [XXX] um zusätzliche Dienstleistungen entsprechende Konzepte des Trading. Dabei wird unter „Trading“ der Prozeß der dynamischen (d.h. zur Laufzeit durchgeführten) Auswahl von passenden Dienstangeboten zu einer vorgegebenen Dienstanfrage verstanden. Diese Dienstanfrage basiert jedoch nicht nur auf einer Spezifikation von Attributnamen und -werten (z.B.: "Kosten : 10.000; Jahr: 1995"), sondern auf der Möglichkeit, komplexe Optimierungskriterien zu definieren ("Kosten < 10.000; Jahr >= 1995).

Das zugrundeliegende Modell des Trading geht davon aus, daß zunächst die Dienstanbieter in offenen verteilten Systemen ihre (Dienst-) Schnittstellen (bzw. Beschreibungen davon) an den Trader exportieren, dann zu einer vorgegebenen Anfrage ein Dienstinachfrager einen „passenden“ Dienst vom Trader importiert und damit der Klient dann eine direkte Bindung zu dem durch den Trader vermittelten Dienstanbieter eingeht. Wichtigste und komplizierteste Teilaufgabe innerhalb der vom Trader durchgeführten Dienstvermittlung ist die *Auswahl eines passenden Dienstangebotes* für eine vorliegende und hinreichend „vollständig“ spezifizierte Dienstinachfrage. Im Zuge der Standardisierung des Traders wurde der Begriff des *Diensttyps* stärker formalisiert. Er faßt folgende Aspekte zusammen: Einen eindeutigen *Typnamen*, der sich zusammensetzt aus einem *Schnittstellentyp* des Dienstes sowie einer Menge von *Dienstattributen*. Diese Dienstattribute sind ihrerseits Name/Wert-Paare.

Als Beispiel sei hier ein Druckdienst angeführt, dessen Diensttyp neben dem Typbezeichner „PrintService_t“ und dem Schnittstellentyp noch weitere Attributtypen umfaßt, z.B.:

```

PaperSize:      enum {A4,A5,Legal,US-Letter}
PagesPerMinute: Int
QueueLength:    Int

```

Server (in der Rolle eines *Exporteurs*) stellen diese Information beim Dienstangebot dem Trader zur Verfügung, während Clients (in der Rolle des *Importeurs*) sie zur Spezifikation des gewünschten Servers nutzen. Die Aufgabe des Traders liegt dabei im *Matching* von Angebot und Nachfrage.

Der Prozeß des Trading

Der Trader setzt nun dieses Klassifikationsprinzip systemtechnisch für die Vermittlung von Diensten um. Zu diesem Zweck bietet er Schnittstellen an für den Importeur, den Exporteur und den Trader-Administrator. Bevor für eine Anfrage des Importeurs eine erfolgreiche Dienstvermittlung durchgeführt werden kann, ist zunächst der Dienstyp des Servers zu registrieren. Über die Verwaltungsschnittstelle des Traders können zu diesem Zweck Daten-, Schnittstellen- und Dienstypdefinitionen eingefügt oder gelöscht werden. Typdefinitionen sind somit Objekte, die zur Laufzeit vom Trader oder seinen Nutzern interpretiert werden können (vgl. z.B. [MML95b, MML95d]).

Nachdem alle erforderlichen Typinformationen registriert wurden, kann jetzt über die *Dienstangebotsverwaltung* das Dienstangebot eines konkreten Anbieters an den Trader exportiert werden. Hierbei erhält der Trader den Dienstypnamen, die Werte verschiedener Dienstattribute sowie weitere Informationen über den Exporteur. Der exemplarische Druckdienst könnte über die Exportschnittstelle etwa folgendes Dienstangebot bereitstellen:

```

ServiceType: PrintService_t
( PaperSize: A4;
  PagesPerMinute: 12;
  QueueLength: 5;
  Category: "/DE/HH/Ponton/LaserJet" )
InterfaceReference = <http://www.ponton-hamburg.de/4711>

```

Jetzt kann die Dienstvermittlung an einen Importeur erfolgen. Über die Import-Schnittstelle wird dem Trader dabei der Dienstyp des Anbieters zusammen mit erwünschten Attributwerten übergeben. Im Beispiel des Druckdienstes könnte folgende Dienstanforderung durch den Exporteur befriedigt werden:

```

ServiceType: PrintService_t
( PaperSize: A4;
  PagesPerMinute: >4;
  Category: "/DE/HH/Ponton/LaserJet" )

```

Zusätzlich zu den Daten des Dienstangebots werden *Policies* wie z.B. *PagesPerMinute>4* spezifiziert, die dem Trader eine Bewertung der verwalteten Dienstangebote erlauben. Weitere Parameter der Dienstanforderung können sich z.B. auf die Suchstrategie des Traders beziehen: Soll ein zufälliges Dienstangebot ausgewählt werden oder das am längsten nicht genutzte oder das erste innerhalb einer Ordnung etc.

Architektur eines Traders

Wie bereits dargestellt, erfordert der Prozeß des Trading eine Registrierung des Dienstyps und mindestens ein zu diesem konformes Dienstangebot, bevor eine Dienstvermittlung über die Import-Schnittstelle durchgeführt werden kann. Da ein Trader sowohl Dienstypdefinitionen als auch auf der Instanzebene Dienstangebote verwaltet, wird üblicherweise eine Trennung in Dienstypmanagement und Dienstangebotsverwaltung vorgenommen. Das DTM verwaltet dabei eine Hierarchie, welche die Subtypbeziehung zwischen Dienstypen repräsentiert. Wurde eine Menge von Einträgen ermittelt, die gemäß dieser Subtyprelation kompatibel zum nachgefragten Dienstyp sind, wird im nächsten Schritt über die Dienstangebotsverwaltung innerhalb des beim Import spezifizierten Kontexts überprüft, welche Dienstangebote als Instanzen zu den ermittelten Typen in Frage kommen. Hierbei werden neben dem Dienstypnamen vor allem auch Dienstattribute und ihre spezifischen Ausprägungen als weiter eingrenzendes Konformitätskriterium verwendet [MML95b]. Dieser Prozeß grenzt die Menge der letztlich resultierenden Dienstangebote weiter ein.

Steht schließlich nach diesem Selektionsprozeß mehr als ein Dienstangebot zur Verfügung, hängt es von der Policy des Traders ab, ob z.B. das erste, ein zufällig ausgewähltes oder ein nach gegebenen Optimierungskriteri-

en (z.B. minimaler Preis) als das „beste“ ermittelte Angebot dem Importeur geliefert wird. Für den Importeur besteht die Wahl einer für den Vermittlungsprozeß sinnvollen Auswahlpolitik, wie z.B. die Optimierung nach einem Dienstattributwert (minimaler Preis).

Bewertung

Der Dienstvermittlungsmechanismus des Trading eignet sich im kommerziellen Kontext des elektronischen Marktes insbesondere bei einem bez. der Produktspezifikation stabilisierten Dienstmarkt. Solche Commodity-Märkte sind durch *Börsensysteme*, wie z.B. Handelssysteme für Wertpapiere, Frachtkapazitäten, Reiseveranstaltungen oder auch Mitfahrzentralen, realisierbar. Für diesen Bereich liefert der Trader einen Mechanismus zur Annäherung an den Zustand der vollständigen Konkurrenz. Für Anbieter, deren Service über die durch Dienstattribute erfaßbare Leistung hinausreicht, besteht allerdings erstens der Nachteil, diese Eigenschaft nicht operabel beschreiben zu können, was sich zweitens negativ auf ihre Innovationsfähigkeit auswirkt. Gerade bei komplexen Produktspezifikationen muß jedoch die Möglichkeit bestehen, auch ohne Dienststypstandardisierung am elektronischen Markt präsent zu sein und die besonderen Vorteile des Dienstes dem Nachfrager gegenüber zu präsentieren.

Ein Broker sollte daher sowohl die Vermittlung und Nutzung von einfach spezifizierbaren – und damit vom Trader vermittelbaren – wie auch komplexe in komplementärer Form unterstützen. Es bleibt dann den Marktteilnehmern überlassen, sich in der einen oder anderen Form zu registrieren.

7.2.3 Zusammenfassung

In diesem Abschnitt wurden einige Business-to-Business-Anwendungen gezeigt, die entweder über das Extranet einzelner Unternehmen oder ausgelagert durch neutrale Dritte realisiert werden können. Als Erkenntnis kann nun abgeleitet werden, daß Extranet-Anwendungen sich allgemein der Internet-Technologie und spezieller dem WWW als Zugangstechnik bedienen. Damit ist zumindest auf der einen Seite immer der Mensch als Bediener und Entscheidungsträger erforderlich.

Diese Einbindung ist erforderlich, da Geschäftsanwendungen nicht in der Lage sind, ad hoc Kommunikationsbeziehungen aufzubauen. Hier mangelt es vor allen an zwei Voraussetzungen: einer *angemessenen Softwaretechnologie* zur raschen Konfiguration von Geschäftsbeziehungen (also eben nicht zur *Kommunikationsbeziehungen*) sowie Standards zur Kooperation zwischen Unternehmen. Beides ist heute zum Teil bereits gegeben, jedoch das eine noch ohne das andere:

Kooperationsstandards sind mit EDI nur bezüglich des Austauschformates von Dokumenten etabliert, jedoch fehlt hier eine Unterstützung zur Ad-hoc-Konfiguration der beteiligten Anwendungen.

Die erforderliche Softwaretechnologie ist ebenfalls am Entstehen, allerdings fehlen hier wiederum Standard-schnittstellen und -prozeduren, um das semantisch korrekte Zusammenwirken von Softwarekomponenten unterschiedlicher Hersteller und Anwender zu erreichen.

Die folgenden Abschnitte beleuchten jeweils diese Fragestellung aus unterschiedlichen Perspektiven und zeigen auf, in welcher Form eine zukünftige Konvergenz dieser unterschiedlichen Technologien nutzbringend sein wird.

7.3 Business Objects

In einer vernetzten Volkswirtschaft verwischen Grenzen zwischen Unternehmen: Historisch bedeutsame Kernbestandteile einer Unternehmung – wie z.B. das Lager – werden heute an Kooperationspartner ausgelagert. Virtuelle Unternehmen zielen sogar darauf ab, für einzelne Aufträge die Konfiguration aller erforderlichen Dienstleistungs- und Fertigungsprozesse ad hoc einzurichten (vgl. Kapitel XXX). Diese Flexibilität ist über Branchen und Wertschöpfungsstufen, aber auch zwischen Unternehmen im Wettbewerb hinweg denkbar.

Diese organisatorische Integration erfordert begleitend eine informationstechnische Vernetzung, so daß die beteiligten Softwaresysteme entsprechend der virtuellen Organisation konfiguriert und abwickelt werden können.

Auch ohne einen solchen Verbund gleich "virtuell" nennen zu müssen, begegnen wir heute einer Reihe von Integrationsformen, die im Kapitel XXX beschrieben sind. Dieses Business-to-Business Electronic Commerce zeichnet sich durch folgende Merkmale aus:

- Es sind vorwiegend Softwarekomponenten bei Handelstransaktionen beteiligt. Der Mensch tritt dabei eher als Konfigurator bzw. Überwacher automatisierter Prozesse in Erscheinung.
- Die unterschiedlichen Geschäftsregeln wechselnder Partner bestimmt die Art und Weise, wie gegenseitige Leistungen auszutauschen sind. Dabei besteht an die Electronic-Commerce-Software die Anforderung, bei wechselnden Geschäftspartnern entsprechend rasch Kompromisse hinsichtlich der neuen Randbedingungen zu treffen.
- Eine Standardisierung ist nicht nur auf der Ebene der Kommunikation erforderlich, sondern vor allem auch im Bereich der Geschäftsprozesse sowie des gemeinsam verwendeten Vokabulars der beteiligten Softwaresysteme.

Die technologische Antwort auf diese Anforderung lautet: *Business Objects*. Solche Softwaremodule zeichnen sich durch die Eigenschaft aus,

- eine *klar abgrenzbares, geschäftliche Funktion* zu repräsentieren. Dies ist z.B. eine Wechselkursstabelle, das Lager, das Hauptbuch oder ein Mitarbeiter.
- ein *Objekt* zu sein. Im Sinne der Objektorientierung bedeutet dies, Daten zu kapseln, Zugriffs und Verarbeitungslogik in Form Methoden zu repräsentieren und teilweise anderen Objekten zugänglich zu machen, sowie durch ein für alle Objekte der gleichen Art gültiges Konzept – die Klasse – gemeinsame Datentypen und Methoden zu definieren.
- *von technologischen Plattformen zu abstrahieren*, d.h., Business Objects sind unabhängig sowohl von der Hardware- als auch von der Betriebssystemumgebung.
- *beliebig verteilbar zu sein*. Neben der Plattformunabhängigkeit steht hier die *Verteilungstransparenz* im Vordergrund. Dies bedeutet, daß eine Konfiguration von Business Objects in beliebiger Weise auf unterschiedliche Rechner innerhalb von oder zwischen Organisationen verteilt werden kann, ohne daß der Anwender einen Unterschied wahrnimmt. In der Realität ist diese Anforderung insbesondere dann gegeben, wenn Geschäftsprozesse über Unternehmensgrenzen hinweg zu integrieren sind. "integrieren" heißt hier: verteilte Business Objects mit einander konfigurieren.
- eine Komponente zu sein. Im Sinne der *Componentware* ist eine Komponente definiert als abgeschlossenes Softwareobjekt, das über die Delegation von Methodenaufrufen mit anderen Komponenten integriert werden kann. Damit werden Softwarekomponenten in Form einer einzelnen Datei geliefert. Eine Komponente trägt Metainformation mit sich, so daß sie vom Softwareentwickler bez. ihrer Funktion und Einsetzbarkeit inspiziert werden kann. Durch die genannten Eigenschaften kann eine Komponente im laufenden Betrieb sofort getestet und eingesetzt werden.
- Schließlich erfordert die Konfiguration von Business Objects die bereits erwähnte Standardisierung der Ausführungsumgebung, von Schnittstellen zwischen Softwaremodulen und des verwendeten Begriffsapparates.

Produkte

Verschiedene Produkte und Standards stehen heute zur Verfügung, um komplexe Anwendungen aus Business Objects zu konstruieren:

- Java Beans
- Die CORBA Business Object Component Architecture
- Enterprise Java Beans
- SAP Business Objects
- Das IBM San Francisco Framework
- Microsoft's Visual-Basic und seine OCXe

In den folgenden Abschnitten wollen wir uns einige dieser Technologien etwas genauer ansehen. Dabei werden wir mit Basistechnologien wie Java und CORBA beginnen, um anschließend zu untersuchen, wie deren Eigenschaften in Architekturen wie BOCA oder Enterprise Java Beans zur Bereitstellung einer Business-Object-Architektur genutzt werden. Anschließend untersuchen wir noch einige proprietäre Produkte und Frameworks, wie z.B. IBM's San Francisco, SAP Business Objects oder Microsoft's Visual Basic.

7.3.1 Java Beans

Daß Java aus der heutigen Welt der Softwareentwicklung nicht mehr wegzudenken ist, zeigen schon die Schwierigkeiten bei der Suche nach Java-Entwicklern: Es gibt keine mehr! Damit sollte es sich auch erübrigen, erneut über alle Vorteile und Eigenschaften von Java als Programmiersprache, Java als Rahmenwerk von Softwaremodulen oder Java als Geisteshaltung im Zeitalter einer Microsoft-beherrschten Welt zu sprechen. Somit nur folgendes in Kürze:

"Plain Java"

Java ist objektorientiert und plattformunabhängig. Java-Anwendungen können ohne Modifikation auf jeder Plattform ausgeführt werden, die das erforderliche Laufzeitsystem – die Java Virtual Machine – zur Verfügung stellt. Diese Plattformen reichen von SmartCards über eingebettete Controller, Personal Digital Assistants, Set-Top-Boxes, PCs, Workstations bis zu Mainframes. Zum erstenmal ist damit eine tatsächlich allgegenwärtige, einheitliche und skalierbare Ausführungsumgebung für eine einzelne Programmiersprache gegeben. Dabei können Java-Module dynamisch geladen und ausgeführt werden. Von der Internet-Standardisierung erbt Java die Verwendung eines einheitlichen Namensraumes über die Verwendung von URLs – ein wesentlicher Beitrag zum Erfolg der Sprache! Dabei ist Java-Code sehr kompakt, so daß über das Netz geladene Module keine unerträglichen Ladezeiten erfordern.

Aber auch für den Programmierer bietet Java Vorteile, die im Vergleich zu C und C++ den Entwicklungsprozeß mindestens um die Hälfte der Zeit verkürzen: Java ist robust gegenüber Programmierfehlern, da diese durch den Entwickler oder das Laufzeitsystem selbst in Form von Ausnahmen abgefangen werden können. Die statische Typisierung von Java-Klassen hilft, Typfehler bereits bei der Kompilation zu erkennen. Den eigentlichen Segen erfährt jedoch der Java-Novize, wenn er feststellt, daß die lästigen Pointer, die ihn einen Großteil seiner C++-Entwicklungszeit kosteten, nun der Geschichte angehören: Ein Objekt wird alloziiert, wenn es benötigt wird und automatisch freigegeben, wenn dies nicht mehr der Fall ist.

Java wird in Form von Bytecode ausgeführt, d.h. der Compiler generiert keinen unmittelbaren Maschinencode, sondern eine Zwischenversion, die mit Hilfe von Interpretern während der Ausführung umgesetzt wird in den tatsächlichen lokalen Code. Dies führt natürlich zu Verzögerungen gegenüber "nativ" kompiliertem C-Code und somit auch einem bislang signifikanten Nachteil von Java: es ist sehr langsam. Dabei hilft auch kein Just-in-Time-Compiler (JIT), der den Bytecode beim Laden sofort in Maschinencode umsetzt (dies dauert natürlich noch länger als das bloße Laden), um ihn anschließend jedoch umso schneller auszuführen (in der Hoffnung daß der Code sooft ausgeführt wird, daß sich der JIT-Prozeß "rechnet"). Als Rettung vor dem Makel der Langsamkeit wird von Sun eine Technologie namens "Hot Spot" angepriesen, um durch dynamische Optimierung des geladenen Codes eine Beschleunigung auf das Niveau von Maschinencode zu erreichen.

Dem Entwickler stellt sich Java als mehrschichtige Architektur dar:

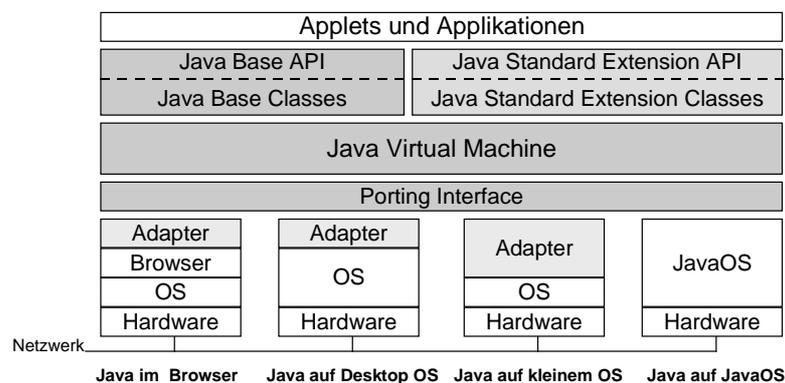


Abb. 36: Die Architektur von Java

Den Dreh- und Angelpunkt dieser Architektur stellt die virtuelle Maschine dar, also der Prozessor, der Java-Bytecode ausführt. Darunter und darüber zerfällt die Architektur in unterschiedliche Alternativen: Um unterschiedliche Hardware- und Betriebssystemumgebungen mit variierendem Funktionsumfang abzubilden, wurden unterschiedliche Adapter entwickelt. Die kann bis zum fast vollständig in Java implementierten Betriebssystem JavaOS reichen. Oberhalb der JVM stehen unterschiedliche *Packages* zur Verfügung, die als Klassenbibliotheken vorgefertigte Java-Klassen enthalten. Einige dieser Packages werden als Bestandteil einer jeden Java-

Umgebung vorausgesetzt (Java Base), während andere zwar standardisiert sind, jedoch nicht notwendigerweise bei jeder JVM erwartet werden können. Beispiele für JavaBase sind Klassen für die Netzkommunikation, GUI-Funktionen oder auch Java Beans. Letztere enthalten z.B. CORBA-, Telefon- und Multimedia-Erweiterungen.

Java Beans ist somit eines von vielen Packages der Kernumgebung von Java. Was ist nun eine Java Bean? Die Dokumentation sagt:

„A Java Bean is a reusable software component that can be visually manipulated in builder tools.“

Zur genaueren Klärung dieser Aussage müssen wir jedoch zunächst verstehen, worin der Unterschied zwischen Java Beans und "normalen" Java-Klassen liegt: Eine Java-Klasse zeichnet sich aus durch eine Anzahl von Methoden und Attributen, die externen Objekten durch Methodenaufrufe zugänglich gemacht werden können. Außerdem kann eine Klasse von einer weiteren erben und verschiedene Interfaces implementieren. Letzteres ist als Versprechen zu verstehen, eine durch Schnittstellendefinition vorgegebene Spezifikation "mit Leben" – d.h. Methoden – zu erfüllen. Wenn nun ein Objekt dieser Klasse zur Laufzeit instanziiert wird, sind alle spezifizierten Methoden aufrufbar. Dabei ist es Sache der Laufzeitumgebung, die erforderliche Klasse, die den Code der Methode beheimatet, dynamisch zu laden. Dies kann ggf. auch über das Netz vom anderen Ende der Welt erfolgen, wenn die Methode von einer anderen Klasse geerbt wurde. Die Wiederverwendung von Code erfolgt somit traditionell durch Erben von der erforderlichen Klasse.

Somit ist die Aussage "Java is a reusable software component" im Prinzip auch für jede ordinäre Java-Klasse gültig.

Eine andere, oben erwähnte Eigenschaft von Komponenten ist die Möglichkeit, sie zur Laufzeit zu inspizieren, d.h. Informationen über die Funktion und Eigenschaft einer Komponente auszulesen. Auch dies ist bereits beim "plain Java" möglich: seit der Version 1.1 des Java Development Kit stehen Methoden zur "Reflexion" zur Verfügung. Unter Reflexion wird die Möglichkeit verstanden, daß Software sich selbst "beobachten" kann: Mit Hilfe von Iterator-Methoden kann zu einem Objekt, das sich in Ausführung befindet, Informationen über seine zugehörigen Klassen, Interfaces, Attribute, Methoden, Parameter etc. erlangt werden. Wird also z.B. eine neue Klasse über das Internet geladen und ein Objekt instanziiert, so kann dem Benutzer diese Information angezeigt werden. Damit erfüllen Standard-Java-Objekte bereits grundlegende Komponenteneigenschaften.

Ein wesentlicher Unterschied besteht jedoch im Prinzip der Wiederverwendung: Durch das Erben von anderen Klassen erfolgt die Wiederverwendung existierender Codes immer zur Entwicklungszeit, denn die Klasse, von der geerbt wird, ist im Quellcode festzulegen. Dies ist jedoch ein schwerwiegendes Hindernis, wenn Module zur Laufzeit konfiguriert und eingebunden werden sollen. Aus diesem Grunde wird für Komponenten das Prinzip der *Delegation* verfolgt. Hierbei werden Methoden, die eine Komponente nicht selbst bearbeiten kann, an eine andere weitergeleitet. Diese Weiterleitung kann zur Laufzeit festgelegt werden, da der Programmierer aufgrund der Inspektion erkennen kann, welche Methoden lokal und welche bei fremden Komponenten zur Verfügung stehen.

Java Beans

Eine Java Bean ist eine normale Java-Klasse, die einem standardisierten Entwurfsmuster folgt und über zusätzliche Klassen verfügt, die Metainformation über die Bean halten. Beans werden zusammen mit dieser Metainformation als Ansammlung von Java-Klassen gebündelt. Dies erfolgt üblicherweise durch Archive, wie sie von WinZIP bekannt sind. Bei Java heißen diese Archive JAR-Dateien (Java Archive), die kompatibel zum ZIP-Format sind. Eine Bean kann neben der eigentlichen Bean-Klasse weitere Klassen besitzen, die mit ihr zusammen als Teil der JAR-Datei ausgeliefert werden, die Bean sollte jedoch von keiner Anwendungsklasse außerhalb dieser Klassen erben, da sonst eine statische Bindung zu externem Code bestehen würde.

Beans kommunizieren über Event-Methoden-Kopplung. Dabei wird bei einer Bean ein Event ausgelöst, z.B. durch eine Benutzerinteraktion oder das Eintreffen eines aktualisierten Börsenkurses. Eine andere Bean, die auf dieses Event reagiert, verarbeitet die betreffende Information. Dabei können beliebig viele Beans auf Events beliebig vieler anderer reagieren.

Beans folgen bei den geschilderten Eigenschaften einem definierten *Entwurfsmuster*. Dies legt fest, wie Attribute und Methoden zu benennen sind, die nicht nur für die Klasse selbst, sondern auch für ihre Benutzer von besonderer Bedeutung sind. Dabei werden sind Beans folgende Muster definiert:

1. Für jedes *Bean-Attribut* steht eine Setter- und eine Getter-Methode zur Verfügung. Die Setter Methode dient dem Schreiben des Wertes und die Getter-Methode dem Lesen. Hat das Attribut beispielsweise den Namen "Color", so sind für die Methoden die Namen "SetColor" und "GetColor" zu verwenden.

2. Für die *Event-basierte Kommunikation* zwischen Beans wird das Muster des "Publish/Subscribe" verwendet: Hierbei sind Events für andere Beans öffentlich (publiziert), so daß diese bei Bedarf ein Event abonnieren können. Auf diese Weise kann auch die N:M-Beziehung zwischen publizierten und abonnierten Ereignissen unterstützt werden. Das Event "neue Ausschreibung" könnte von Beans mehrerer Zulieferer abonniert werden, während jeder Zulieferer die Event mehrerer Kunden abonniert. Auf der Ebene der Programmierung erfolgt das Abonnieren eines Events durch das Registrieren eines "Listeners" bei der Bean, die das Event generiert. Natürlichsprachlich also: "Kunde, ich möchte mich bei Dir bez. der Ausschreibung von Aufträgen registrieren". Formalisiert programmiert sich dies z.B. wie folgt: `KundenObjekt.addAusschreibungListener(AusschreibungListener l)`. `AusschreibungListener` ist dabei ein Objekt des Zulieferers, das im Falle eines Ausschreibungs-Events mit einem Event-Objekt vom Typ "Ausschreibung" aufgerufen wird. Will der Zulieferer diese Beziehung beenden, kann er mit `RemoveAusschreibungListener(AusschreibungListener l)` sein Listener-Objekt wieder aus der Abonnentenliste des Kunden entfernen.
3. *PropertyChange-Events*. Neben solchen Events auf der Anwendungsebene, sind einige bereits vorgefertigt. Diese können abonniert werden, um das Ändern von Attributen bei anderen Beans zu melden. In unserem Beispiel könnte die Frist zum Einreichen von Angeboten verlängert werden. Das betreffende Datum liegt beim Kunden als Bean-Attribut vor. Wenn dieses nun mit `addPropertyChangeListener(...)` abonniert wird, kann der Kunde im Falle einer Änderung des Datums automatisch benachrichtigt werden.
4. ...

Das Beans-Entwurfsmuster

Folgende Benennung muß vom Bean-Entwickler eingehalten werden, damit die betreffenden Bestandteile vom Entwicklungswerkzeug automatisch als Teile der Bean erkannt werden können:

```
public void set<PropertyName> (<PropertyType> value );
public <PropertyType> get <PropertyName> ();
public void add<EventName>Listener(<EventName>Listener l );
public void remove<EventName>Listener(<EventName>Listener l);
public void addPropertyChangeListener(PropertyChangeListener l );
```

Die folgende Graphik visualisiert die Erweiterungen einer Bean-Klasse, die schließlich Java Beans ausmachen:

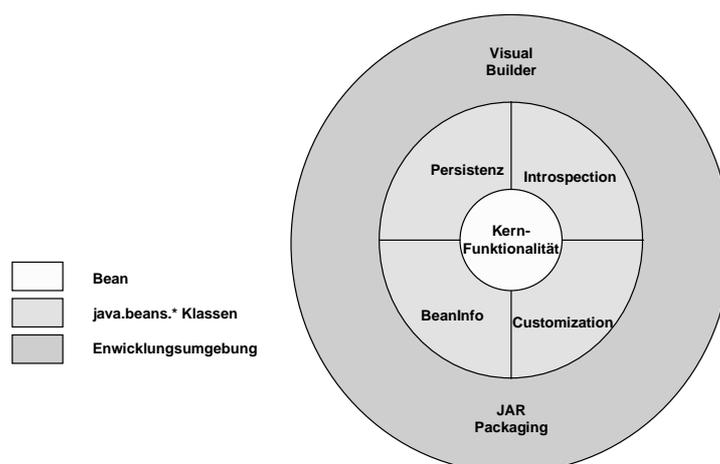


Abb. 37: Bestandteile des Java-Bean-Framework

Die Kernfunktionalität umfaßt die Bereiche Reflexion und Event-Handling. Hier ist es die Verantwortung des Programmierers, die erforderlichen Entwurfsmuster einzuhalten.

Der zweite Ring ist bereits optional. Als Package der Standard-Laufzeitumgebung von Java bieten Beans folgende Erweiterungen zur:

- *Introspection.* Im Beans-Package stehen zusätzliche Klassen zu Verfügung, mit deren Hilfe aussagekräftigere Metainformation an eine Bean gekoppelt werden kann. So lassen sich Events, Methoden, Attribute etc. aufzählen und dazu vom Entwickler eingetragene Informationen abrufen. Diese Informationen können z.B. Texte und Beschriftungen sein, die von einem Entwicklerwerkzeug angezeigt werden. Anstelle des Event-Namen "Ausschreibung" könnte hier beschrieben sein, für welche Produkte Ausschreibungen durchgeführt werden. Als Einstiegspunkt in die Metainformation steht die Klasse BeanInfo zur Verfügung, von der zu weiteren Deskriptor-Klassen verzweigt werden kann.
- *Persistenz.* Da eine Bean für eine längere Zeit im Hauptspeicher verankert werden kann, ist es sinnvoll, ihren Zustand so zu sichern, daß die Bean nach einem Crash oder einem gezielten Auslagern wieder restauriert werden kann. Dazu sind Mechanismen zur Speicherung des Bean-Zustands in einer Datenbank erforderlich.
- *Customization.* Metainformation einer Bean wird von Entwicklungswerkzeugen in ihrer jeweiligen Standardrepräsentation dargestellt. Wenn der Bean-Entwickler jedoch diese Information in einer anwendungsge-rechten Form darstellen möchte, so muß er die Darstellung durch eigenen Code vornehmen. Dieser Customizer-Code ist ebenfalls an die Bean gekoppelt und wird aufgerufen, wenn die Entwicklungsumgebung erkennt, daß Customizer definiert wurden. Beispiele für Customizer sind etwa die Visualisierung als Thermometer für einen Temperaturwert oder die noch verbleibenden Tage bis zur Deadline der Ausschreibung als Sanduhr. Auch die Darstellung der gesamten Bean kann durch einen Customizer übernommen werden. Hier könnte eine 3D-Darstellung oder eine ergonomischere Ein-/Ausgabe der Attributwerte eingebunden werden.

Die Gesamtheit dieses zusätzlichen Java-Code wird zusammen mit den Anwendungsklassen der Bean in einer JAR-Datei verpackt. Quasi als "Beipackzettel" wird dem Archiv noch eine kleine Textdatei, das *Manifest*, beigelegt, die definiert, ob es sich bei der betreffenden JAR-Datei tatsächlich um eine Bean handelt. Dabei kann auch der Name der Bean-Klasse festgelegt werden, wenn diese nicht dem Namen der JAR-Datei entspricht.

Schließlich ist die Bereitstellung einer Bean wenig sinnvoll, wenn sie nicht sinnvoll in Entwicklungsumgebungen integriert wird. Diese sollte eine neue Bean dynamisch laden und in einem Auswahlmenü zur Verfügung stellen. Ferner sollte sie das Instanzieren und Integrieren einer Bean vereinfachen. Die Mutter aller Bean-Werkzeuge, die *Beanbox* der Bean Development Kits von JavaSoft, erlaubt erstmalig die Komposition von Anwendungen nach dem Prinzip des "Drag'n'Drop". Beans können hierbei aus einem Menü auf die Desktop-Oberfläche der BeanBox gezogen werden. Dadurch werden sie unmittelbar ausgeführt, d.h. eine Unterscheidung zwischen Entwicklungs- und Testmodus entfällt. Ebenfalls im laufenden Betrieb können Beans durch Editoren ihrer Attributwerte konfiguriert werden. Die Abbildung zwischen Events und Methoden erfolgt durch das Auswählen des Events aus einem Kontextmenü der Ausgangs-Bean und anschließendes Ziehen einer Verbindung zur Ziel-Bean, bei der wiederum über ein Kontextmenü die korrekte Zielmethode auszuwählen ist. Als Ergebnis kann die Kommunikation sofort im Ausführungsmodus getestet werden.

Heute hat sich bereit ein Bean-Komponentenmarkt etabliert, der zwar vom Volumen her noch nicht mit dem OCX-Markt im Bereich des Active-X vergleichbar ist, aber dennoch eine entsprechende Reife der Produkte entwickelt hat [XXX URLs angeben].

Bedeutung von Java Beans im B2B-Commerce

Als minimale Grundlage bietet Java bereits die Möglichkeit, Software verteilt zu entwickeln und gemeinsam ad hoc zu nutzen: Unternehmen stellen ihre jeweiligen Software-Systeme anderen Geschäftspartner als Packages zur Verfügung, so daß deren Programmierer in die Lage versetzt werden, Systeme beider Unternehmen zu integrieren. Ökonomisch kann dies nur sinnvoll sein, wenn die "Economies-of-Scale" dies rechtfertigen – also nur bei Aufwiegen des hohen Entwicklungsaufwands durch hohe Nutzungsintensität. Hiermit befinden wir uns jedoch wieder in der EDI-Problematik, da in einer Welt des schnelleren Wandels diese Intensität immer weiter abnimmt.

Java Beans helfen, einen Schritt weiter in Richtung Adhocracy zu gehen. Hier ist es nicht mehr der Java-Programmierer, der die Softwaresysteme integriert, sondern der Benutzer der Beanbox. Das Abonnieren eines Ausschreibungs-Events wird damit reduziert zum Verdrahten von Events und Methoden. Neue Kunden lassen sich rasch abonnieren, neue Verarbeitungsformen für diese Events müssen nicht mehr in Eigenregie entwickelt, sondern können von externen Bean-Entwicklern hinzugekauft werden. Dies spart Entwicklungsressourcen und "Time-to-Market".

Aber einige wichtige Voraussetzungen wurde bei der technischen Betrachtung zuvor vernachlässigt:

- Events und Methoden müssen syntaktisch und sematisch abbildbar sein.

- Ein Geschäft besteht nicht nur aus der Kommunikation von Events. Auch die Regeln und Rollen, in denen ein Unternehmen Beziehungen zu anderen eingeht, sind so vielfältig, daß sie nicht durch das "Strippenziehen" zwischen Geschäftspartnern abgedeckt werden können.
- Es fehlt noch an Designwerkzeugen, die existierende Komponenten so integrieren, daß daraus ein vollständiger, sinnvoller und an individuelle Belange anpaßbarer Geschäftsprozeß entsteht.
- Schließlich besteht die Welt noch nicht ausschließlich aus Java Beans. Die Integration von Legacy-Systemen, die in C, COBOL, Fortran etc. entwickelt wurden wird sich auch in der näheren Zukunft nicht durch Neuentwicklung vermeiden lassen.

Dennoch kann man davon ausgehen, daß Java Beans als eine der Säulen zukünftiger Business-to-Business-Integrationen eingesetzt werden kann.

7.3.2 Enterprise Java Beans

Enterprise Java Beans (EJB) ist ein Standard, der von Sun unter maßgeblicher Beteiligung von IBM, Oracle und anderen im März 1998 als Spezifikation verabschiedet wurde. EJBs leben im Gegensatz zu Java-Applets auf der Server-Seite und werden dort in einer Laufzeitumgebung verwaltet. EJBs lassen sich – ähnlich den Stored Procedures bei SQL – auf den Server hochladen und ausführen. Die Ausführungsumgebung umfaßt einen Transaktionsmonitor, der die Atomarität, Konsistenz, Isolation und Dauerhaftigkeit der Ausführung von EJBs sicherstellt. Dies bezieht sich vor allem auch auf die Daten, auf die EJBs zugreifen. Folglich ist es nur natürlich, daß Datenbankanbieter wie IBM und Oracle in der EJB-Entwicklung involviert sind. Weitere Eigenschaften der EJB-Ausführungsumgebung sind Nebenläufigkeitskontrolle und eine Sicherheitsunterstützung, die EJBs entsprechend ihren Rechten und Authentisierungen in der Ausführung beschränken kann. EJB bietet CORBA-Interoperabilität, so daß eine standardisierte Kommunikation mit Anwendungen außerhalb der EJB-Ausführungsumgebung gesichert ist.

Damit wurden wesentliche Funktionen, die für einen großen Teil aller Geschäfts-Applikation erforderlich sind, in einheitlicher, produktunabhängiger Form ausgelagert. Der Anwendungsentwickler kann sich damit auf die Geschäftslogik seiner Anwendung konzentrieren.

Enterprise Java Beans sind speziell für die Nutzungsform auf der Serverseite zugeschnitten: Hier steht die graphische Darstellung der Bean nicht im Vordergrund und damit auch nicht ihr Konfigurieren über die GUI-Schnittstelle. Stattdessen ist die EJB ein Dienstleister, der auf Methodenaufrufe der Clients reagiert und selbst nicht notwendigerweise Events generiert. Server-Applikationen besitzen üblicherweise eine hohe Economy-of-Scale, d.h., hier kann es sinnvoll sein, die Bean mit mehr Aufwand in ihre Umgebung zu integrieren; daher ist sie mit zusätzlicher Metainformation versehen, die nach der EJB-Spezifikation als "Vertrag" bezeichnet wird. Ein solcher Vertrag legt fest, welche Standardschnittstellen die EJB implementiert. Diese Schnittstellen betreffen beispielsweise das Sitzungsmanagement, die Aktivierung einer EJB über Factory-Objekte oder Sicherheitsanforderungen, wie z.B. die Authentisierung zugreifender Clients.

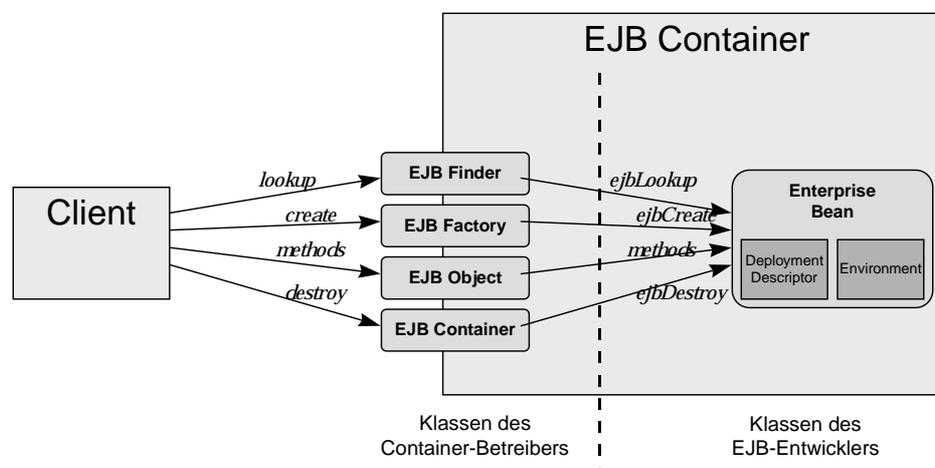


Abb. 38: Integration von Enterprise Java Beans in die Ausführungsumgebung des Containers

Das organisatorische Modell sieht bei EJBs folgende Rollen vor:

- *Entwickler von EJBs.* Diese Rolle nimmt ein Softwareunternehmen oder der Anwender selbst ein. EJBs können im Auftrag entwickelt oder als Produkt auf dem Komponentenmarkt angeboten werden.
- *EJB-Installateur.* Diese Rolle entspricht dem SAP-Beater, der die bestehende EJB in die Umgebung des Container-Betreibers einbindet und für andere Anwendungen bereitstellt.
- *Container-Anbieter.* Diese Rolle nehmen Unternehmen ein, die die EJB-Ausführungsumgebung in ihre Produkte integrieren. Beispiele sind Oracle und IBM mit entsprechenden Erweiterungen ihrer Datenbanksysteme.
- *Betreiber von EJB-Servern.* Der Server-Anbieter läßt EJBs so vom Installateur zusammenstellen, daß sie in einem sinnvollen Kontext benutzt werden können. Je nach Geschäftsmodell kann er auch Dritten zur Verfügung stehen, daß sie seinen Server zur Bereitstellung ihrer EJBs nutzen.
- *Anwendungsentwickler.* Der Anwendungsentwickler programmiert Client-Anwendungen für EJBs. Dabei kann dies ein Java-Applet sein, das vom Benutzer geladen wird oder eine weitere Server-Anwendung, die ihrerseits durch andere Clients zugegriffen wird.

Das Ausschreibungsbeispiel

Greift man entsprechend diesem Rollenmodell unser Beispiel für Ausschreibungen von Aufträgen wieder auf, kann man sich die EJB als Bestandteil des Datenbankservers auf der Kundenseite vorstellen. Der Kunde ist also der Betreiber des EJB-Servers. Autorisierte Anbieter sind in der Lage, Methoden der EJB aufzurufen, um Ausschreibungsinformationen abzurufen. Dabei prüft die EJB-Umgebung anhand von Zertifikaten, wer zugreift und ob eine Berechtigung besteht. Diese Funktion wurde vom Installateur für die spezielle Anwendung eingerichtet. Die Ausschreibungssoftware ist von einem freien Softwareentwickler programmiert worden.

Die erforderliche Client-Software kann dynamisch vom Zulieferer heruntergeladen werden. Zusätzlich ist denkbar, daß Angebote in die Datenbank des Kunden geladen werden sollen. Hier kommt die Transaktionsunterstützung der EJB zum Tragen, da dem Kunden durch ein erfolgreiches "Commit" mitgeteilt werden kann, daß das Angebot dauerhaft gespeichert wurde. Diese Funktion muß nicht vom EJB-Entwickler programmiert werden.

Zukünftige EJB-Anwendungen sind im Zusammenhang mit folgenden Technologien und Produkten vorstellbar bzw. geplant:

- Transaktionsmonitore, wie z.B. IBM TXSeries (CICS and Encina) oder Tuxedo.
- Component Transaction Server, wie z.B. Sybase Jaguar CTS oder Microsoft Transaction Server.
- CORBA-Plattformen, z.B. Inprise's VisiBroker/ITS oder Iona's Orbix/OTM.
- RDBMSs, wie Oracle 8i oder IBM DB2.
- Web Server, wie z.B. der Java Web Server, Netscape's Enterprise Server, oder Oracle's Web Application Server.

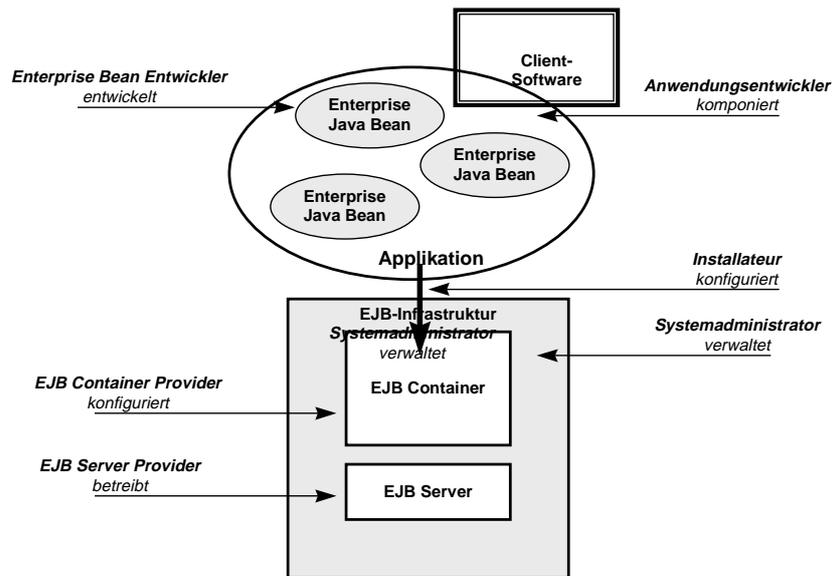


Abb. 39: Organisatorisches Modell bei Enterprise Java Beans

Abb. XXX illustriert den Zusammenhang zwischen verschiedenen EJB-Komponenten, die von Teilnehmern in unterschiedlichen Rollen beigetragen werden. Ein "traditioneller" Anwendungsentwickler wird jetzt zum Enterprise Bean Entwickler. Hier findet Programmierung in Java statt. Ein Anwendungsentwickler selektiert EJBs und komponiert sie zu komplexeren Anwendungen. Diese Konfiguration findet als Definition von Geschäftslogik und Verfahrensregeln für die EJB statt. Dabei sind Aufgaben der Datenspeicherung, der Nebenläufigkeitskontrolle und Transaktionalität ausgespart – diese werden durch die EJB-Infrastruktur des Anwenders in einheitlicher Form bereitgestellt.

Bei EJBs soll diese Komponierbarkeit durch vordefinierte Entwurfsmuster und Namenskonventionen erreicht werden. Dies schränkt zwar die Freiheit der Anwendungsarchitektur einer Software ein, erlaubt aber andererseits dem Entwickler, einheitliche Annahmen bez. der Infrastruktur und ihrer Anwendungen zu machen.

Zwei wesentliche Entwurfsmuster lassen sich bei EJBs unterscheiden, um verteilte, objektorientierte Anwendungen zu entwickeln: den sitzungsbasierten Ansatz und den persistenter Objekte. Im ersten Fall wird für jeden Client ein dediziertes Objekt (die Sitzungs-Bean) erzeugt, das als Stellvertreter des Client gegenüber der EJB agiert. Die Lebensdauer des Sitzungsobjekts wird durch den EJB-Server determiniert und endet in der Regel mit dem Ende einer Client/Server-Sitzung. Nach dem Entwurfsmuster "Persistentes Objekt" repräsentiert das Objekt einen Ausschnitt aus der Datenbank und stellt Operationen zur Manipulation der Daten bereit (Entity Bean). Persistente Objekte werden von mehreren Client genutzt. Die Lebensdauer eines persistenten Objekts hängt von der der Daten ab.

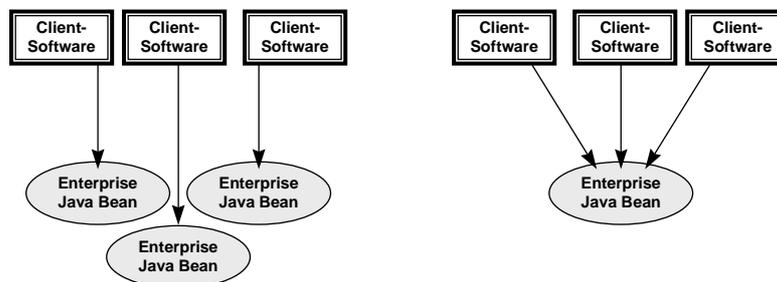


Abb. 40: Sitzungs- und Entity-Beans

7.3.3 Die CORBA Business Object Component Architecture

Die Common Object Request Broker Architecture (CORBA) hat sich heute zur herstellerneutralen Kommunikationsplattform zwischen verteilten Anwendungen entwickelt. In der Literatur ist CORBA Gegenstand etlicher Veröffentlichungen aus dem technischen oder Managementbereich. Aus diesem Grund sollen die CORBA-

Architektur und ihre Basisstandards hier nur am Rande betrachtet werden. CORBA wird dabei als ein existierender Mechanismus vorausgesetzt, der es erlaubt, verteilte Objekte, die in unterschiedlichen Programmiersprachen entwickelt wurden, so zu integrieren, daß eine einheitliche Sicht auf die Gesamtheit aller Objekte, ihre Kommunikation, die Definition ihrer Schnittstellen sowie auf Grundfunktionen, die eine beteiligte Plattform zur Verfügung stellen muß, gegeben ist.

Die Business Object Component Architecture (BOCA) ist als Erweiterung von CORBA zu verstehen. Dies ist zum einen eine *Spezialisierung*, d.h. CORBA wird nur zur Kooperation von Business Objects um zusätzliche Funktionen ergänzt. Zum anderen liegt mit der BOCA eine grundlegende Erweiterung von CORBA vor: Erstmals wird die Modellierung von Geschäftsprozessen als Teil der CORBA standardisiert. Ferner wird die zuvor eher an syntaktischen Merkmalen wie Methodensignaturen und Attributtypen orientierte Schnittstellendefinitionssprache IDL wesentlich erweitert.

Mit der BOCA steht damit ein mächtiges, aber auch sehr komplexes Rahmenwerk zur Business-to-Business-Integration zur Verfügung. Im folgenden soll dieser Themenkomplex "bottom-up" ausgehend von CORBA über ihre BOCA-Erweiterung bis hin zur vollständigen Modellierung und Umsetzung einer Business-to-Business-Integration behandelt werden.

CORBA

CORBA ist eine von der Object Management Group standardisierte Middleware-Architektur zur Kommunikation zwischen verteilten Objekten. Die wesentlichen Eigenschaften der CORBA sind im einzelnen:

- *Unterstützung sprachunabhängiger Schnittstellendefinitionen.* CORBA erlaubt es, Programme, die in unterschiedlichen Programmiersprachen entwickelt wurden, über einen einheitlichen Kommunikationsmechanismus zu integrieren. Dazu definierte die OMG eine Schnittstellendefinitionssprache IDL (Interface Definition Language), mit deren Hilfe Objektschnittstellen beschrieben werden können. Eine IDL-Spezifikation kann anschließend über entsprechende Generatoren in Programmcode der jeweiligen Zielsprache transformiert werden. Dabei wird natürlich nicht die Objektfunktionalität erzeugt, sondern nur der Code, der erforderlich ist, Methodenaufrufe vom einen Rechner im Netz zu dem, auf dem sich das Objekt befindet, zu transportieren. Als Zwischeninstanzen treten bei dieser Kommunikation ORBs (Object Request Broker) auf, welche die Verbindung zum Server-Objekt herstellen und die Kommunikation unterstützen. Das verwendete Kommunikationsprotokoll IIOP (Internet Inter-ORB Protokoll) ist dabei sprachunabhängig, so daß beispielsweise das aufrufende Objekt in Java und das Server-Objekt in COBOL geschrieben sein kann.
- *Transparente Verteilung von Objekten.* Objekte werden durch Objektreferenzen identifiziert, die nicht die Kenntnis des aktuellen Rechners, auf dem sich das Objekt befindet, voraussetzen. Mit Hilfe eines Namensdienstes wird die Auflösung der Objektreferenz durch das CORBA-System durchgeführt.
- *Standardisierung unterschiedlicher Objektklassen.* Der ORB wird zur Verbindung zwischen Objekten eingesetzt. Damit ist noch nicht festgelegt, von welchem Typ die kommunizierenden Anwendungsobjekte sind. Diese Objekte können speziell für eine Anwendung entwickelt, für horizontale oder vertikale Einsatzbereiche vorgefertigt sein oder schließlich als fester Bestandteil einer CORBA-Implementierung mitgeliefert worden sein. Diese Unterscheidung geht einher mit der Standardisierung von Anwendungsobjekten gemäß der Object Management Architecture (OMA)

Die OMA (Abb. XXX) unterscheidet drei unterschiedliche Arten von Objekten:

- *CORBA Services* sind Standardobjekte, die für allgemeine Zwecke wie der dauerhaften Speicherung von Objekten dienen.
- *CORBA Facilities* werden eingesetzt für horizontale, funktionsspezifische (Benutzerschnittstellen, Anwendungs- und Systemmanagement) oder vertikale, branchenspezifische Standards (Gesundheitswesen, Finanzwesen, Telekommunikation).
- Schließlich sind *Application Objects* die Objekte, die der Anwendungsprogrammierer einer CORBA-Anwendung selbst entwickelt.

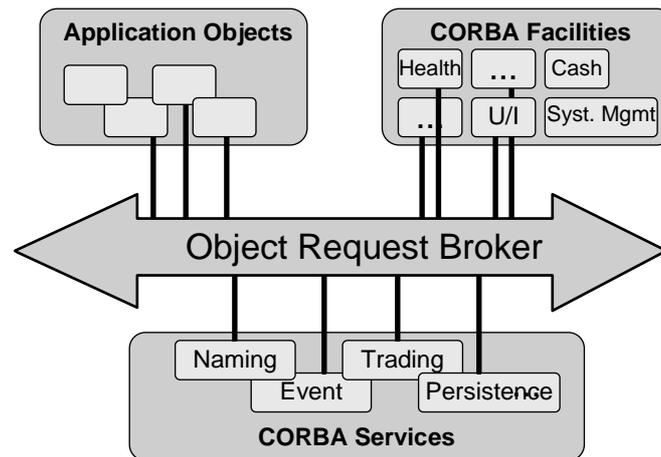


Abb. 41: Die Object Management Architecture

IDL-Spezifikationen und der Stub-Generator

Eine IDL-Schnittstellendefinition beschreibt Methoden und Attribute eines Objektes. Dabei sind Attribute über Setter- und Getter-Methoden modifizierbar. Anhand von Objektschnittstellen definieren IDL-Spezifikationen die Funktionalität von Objekten. Dabei können Schnittstellen voneinander erben. Ein Objekt, das eine bestimmte IDL-Schnittstelle implementiert, muß daher auch alle von ihr geerbten Schnittstellen implementieren. IDL erlaubt ferner die Schachtelung von Modulen und Schnittstellendefinitionen. Module können dabei neben Attributen weitere Module oder Schnittstellendefinitionen enthalten.

Als Beispiel stelle man sich vor, daß die Schnittstellen "EventSubscriber" und "EventPublisher" von einer Schnittstelle "EventAwareObject" geerbt werden. Ein Objekt, das "EventAwareObject" implementiert, muß auch alle Methoden und Attribute der ersten beiden Schnittstellen implementieren.

Mit Hilfe eines Stub-Compilers werden aus den Spezifikationen einer IDL-Datei Programmfragmente in unterschiedlichen Sprachen generiert. Diese Fragmente helfen einerseits als *Client-Stub*, die Aufrufchnittstelle des entfernten Objekts zu simulieren und andererseits, als *Skeleton* den Server mit dem Orb zu integrieren. Wenn ein entfernter Methodenaufwurf ausgeführt wird, so bedeutet dies auf der Client-Seite, daß die generierte Methode des Stubs aufgerufen wird. Dieser leitet die Parameter an den lokalen ORB weiter und von dort aus an den Ziel-ORB des Server-Objekts. Hier wird mit Hilfe des Skeletons der eigentliche Methodenaufwurf an das Objekt ausgeführt. Nach Beendigung der Methode sendet der Server-Orb das Resultat umgekehrt an den Client zurück.

CORBA Services

Ein spezieller CORBA Service ist das *Interface Repository*. Dieser Service erlaubt es, den Inhalt von IDL-Spezifikationen so zu repräsentieren, daß online auf Schnittstellenbeschreibungsobjekte zugegriffen werden kann. Das Navigieren durch das Interface Repository ermöglicht es einer Anwendung, alle Informationen der entsprechenden IDL-Spezifikation abzufragen. Interface Repository und IDL-Datei sind somit lediglich zwei unterschiedliche Repräsentationsformen für die gleiche Information.

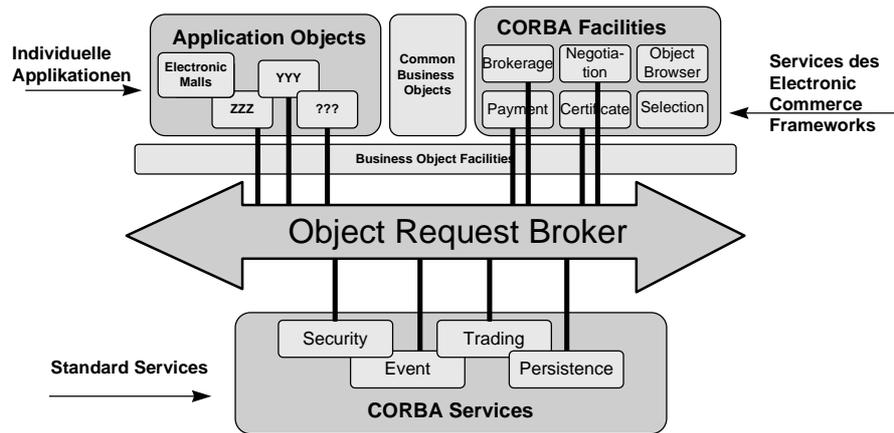


Abb. 42: Erweiterungen von CORBA für Business Objects

Die Business Object Component Architecture

Basierend auf der Object Management Architecture von CORBA, wird mit der BOCA versucht, ständig wechselnde und sich wandelnde Geschäftsprozesse so abzubilden, daß eine flexible Kooperation über Unternehmensgrenzen hinaus ermöglicht wird. Dabei wurde für diesen Zweck eine spezielle CORBA Facility definiert: die *Business Object Facility* (BOF), durch die eine Plattform zur Modellierung und Ausführung von Business Objects zur Verfügung steht. Diese Plattform bietet jedoch noch nicht ein einziges "Nutzobjekt" an, sondern lediglich Mechanismen zur Verwaltung und Beschreibung von Business Objects. Die eigentlichen Business Objects werden erst für eine spezielle Anwendung konfiguriert. Dabei unterscheidet man generell zwischen *Common Business Objects* (CBOs) und *Specific Business Objects* (SBOs). Erstere werden als Rahmenwerk von Softwareanbietern wie IBM, Oracle etc. bereitgestellt. Dabei sind CBOs im Rahmen der BOCA standardisiert, so daß hier noch keine Möglichkeiten zur funktionellen Diversifikation bestehen. Erst im Bereich der SBOs können unternehmensspezifische Anpassungen durch "Customizing" vorgenommen werden. Diese Business Objects sind herstellereinspezifisch (IBM, Oracle o.ä.), funktionenspezifisch (Finanzwesen, Produktion, Dokumentenmanagement) oder kundenspezifisch. In jedem Fall setzen sie jedoch die Anwesenheit der CORBA-Plattform, der BOF sowie der CBOs voraus. Abb. XXX stellt diese Bausteine der BOCA in ihrem architekturellen Zusammenhang dar.

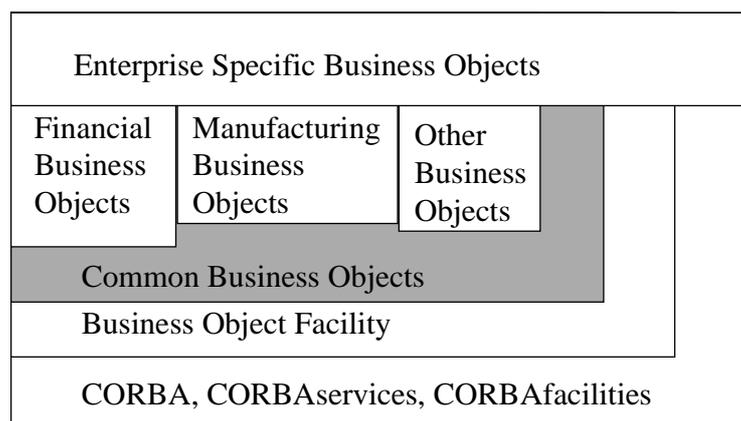


Abb. 43: Bausteine der BOCA

Neben solchen statischen Zusammenhängen der BOCA sind etliche weitere Fragen zu klären, bevor ein Unternehmen in die Lage versetzt wird, auf der Basis von Business Objects mit anderen zu kooperieren. Im wesentlichen sind folgende Probleme zu lösen:

- Wie kann dieses Modell auf die BOF-Infrastruktur abgebildet werden?
- Wie kann das Gesamtwerk der Business Objects für einen speziellen Anwendungsfall modelliert werden?
- Wie können Unternehmen auf der Basis von Business Object flexibel "zusammengeschaltet" werden?

■ Wie kann dabei Technologieunabhängigkeit weitestgehend aufrechterhalten werden?

Antworten auf diese Fragen sollen nun im einzelnen anhand der BOCA erläutert werden. Wir werden später zu diesen Fragen zurückkehren, wenn es darum geht, andere Business-Object-Architekturen zu vergleichen.

Definitionen

Business Objects sind CORBA-Objekte und damit über einen ORB über das Netz identifizierbar und nutzbar. Ein Business Object repräsentiert einen Gegenstand oder Prozeß eines Geschäftsbereichs. Diese können beispielsweise Aufträge, Kunden, Abteilungen, Produkte oder Projekte sein. Ein Business Object besitzt eine eindeutige ID, mit der es an einem bestimmten Ort gekoppelt ist. Ein Business Object kann damit nicht kopiert, sondern nur verschoben werden, so daß die ID des Objektes nicht dupliziert wird. Anhand der ID kann es persistent in einer Datenbank gespeichert und gesucht werden. Schließlich gehören Business Objects einem Typ an, der festlegt, über welche Attribute, Methoden, Events, Rollen etc. sie verfügen. Business Objects können Eigenschaften und Verhalten von anderen erben.

Neben Business Objects existieren *abhängige Typen* (Dependent Types), deren Objekte nicht eindeutig identifizierbar sind, sondern nur in Verbindung mit einem Business Object verwendet werden können. Attribute eines Business Objects sind z.B. von einem abhängigen Typ. Eine Adresse als Bestandteil eines Objekts vom Typ "Kunde" gehört dem abhängigen Typ "Adresse" an. Ferner sind standardisierte Typen wie Währung, Farben, Gewichte etc. abhängige Typen, die als Teil der BOCA festgelegt werden. Ferner sieht die BOCA *Commands* (Skripte), Konstanten usw. als weitere Typen dieser Kategorie vor.

Unter *Features* werden alle Bestandteile eines Business Objects zusammengefaßt, die seinen Typ ausmachen. Diese Bestandteile sind Attribute, Beziehungen, Zustände, Operationen und Appliances. Neben diesen Features sind bei der BOCA noch Feature-Parameter definiert, die helfen, eine Spezifikation von Business Objects weiter zu verfeinern. So ist z.B. die Kardinalität einer Beziehung ein Feature-Parameter.

Die Gesamtkonstellation aller Features konstituiert einen *Vertrag*, den der Besitzer des Business Objects anbietet. Dabei setzt sich dieser Vertrag aus Rechten und Pflichten in Form von Features zusammen. Der Begriff des "Vertrags" ist hierbei also sehr formal im Sinne einer technisch/organisatorischen Spezifikation und weniger im juristischen Sinne zu verstehen. Wir werden uns später noch im Bereich des Online-Contracting mit juristischen Verträgen befassen.

Unter einer Business System Domain (BSD) ist bei der BOCA ein verteiltes Objektsystem zu verstehen, das einen Geschäftsbereich repräsentiert und unter seiner Kontrolle ausgeführt wird. Der Geschäftsbereich ist dabei verantwortlich für die zuverlässige, konsistente und robuste Ausführung aller Business Objects seiner BSD. Diese kann ein kleines Unternehmen oder eine Abteilung in einem größeren umfassen.

BSD können eine Föderation eingehen, d.h. ihre Geschäftsbereiche nutzen die Business-Object-Infrastruktur für den gezielten Zusammenschluß ihrer Funktionen. In der BOCA stehen als Teil der BOF generelle *Adapter-Objekte* zur Verfügung, mit deren Hilfe einer fremden BSD Zugang zu Objekten der eigenen verschafft werden kann. Adapter können dazu für individuelle Business Objects durch die Bildung von Subklassen verfeinert werden. Im Gegensatz zu Proxies bei CORBA verfügen Adapter jedoch über eigene Logik, so daß sie z.B. zur Plausibilitätsprüfung von Methodenparametern verwendet werden können. Als Beispiel kann man sich ein Business Object "AuftragsErfassung" beim Zulieferer vorstellen, das mit Hilfe eines "AuftragsErfassungAdapter" externen Kunden zugänglich gemacht werden kann. Diese erzeugen sich dazu einen Adapter in ihrer eigenen BSD und können dessen Funktion in ihr lokales Warenwirtschaftssystem integrieren.

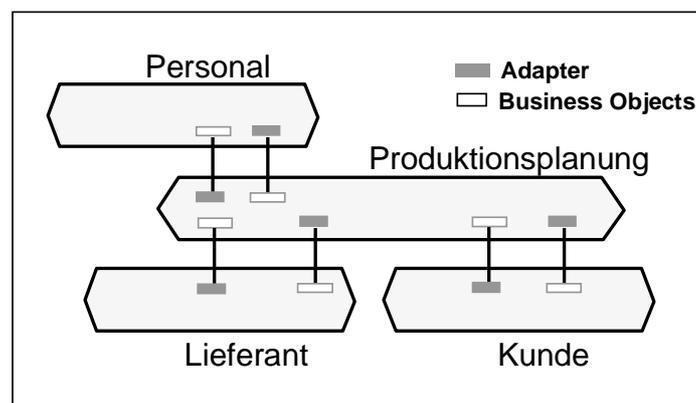


Abb. 44: Adapter zwischen Kunden und Lieferanten

Typmanager dienen zur Verwaltung von Business Objects des gleichen Types. Beispielsweise wird ein Objekt "Customer-Typmanager" genutzt, um ein neues Kundenobjekt zu instanzieren. Neben dieser, bei verteilten Objektsystemen auch *Factory* genannten, Funktion besteht die Aufgabe eines BOCA-Typmanagers in der Verwaltung des Objektes während seiner gesamten Lebensdauer. Dazu zählen folglich auch Funktionen der Ein- und Auslagerung des Objekts in die Datenabank, der Verwaltung der Gesamtzahl an Objekten des Managers sowie Bereinigungsarbeiten, wenn das Objekt wieder gelöscht werden soll.

Auch bei der BOCA wird ein *Event-Modell* unterstützt, das dem Publish/Subscribe-Prinzip folgt. Es entspricht im wesentlichen dem Eventmodell von Java Beans, d.h. eine beliebige Anzahl Abonnenten können sich jeweils bei einer beliebigen Anzahl von Event-Produzenten registrieren. Dieses läßt sich abbilden auf den CORBA Event-Service, der als Teil der CORBA-Basisarchitektur zur Verfügung steht. Als Produzenten eines Events dienen die Features von Business Objects (Events, Beziehungen, Attribute, Zustände etc.).

Die Wiederverwendbarkeit von Business Objects ist häufig dadurch eingeschränkt, daß zusätzliche Funktionalität nur durch explizites Programmieren einer Spezialisierung von Standardobjekten hinzugefügt werden kann. In der BOCA dienen *Appliances* als Mechanismus, diese Beschränkung zu umgehen. Ähnlich einem Plug-In, können Appliances zur Laufzeit über eine generische Schnittstelle an ein Objekt "angeflascht" werden, so daß die speziellen Funktion der Appliance die des Objektes ergänzt oder modifiziert. Als Beispiel sind Regeln denkbar, die beim Objekt "Lagerbestand" das Event "Mindestbestand Unterschritten" auslösen. BOCA definiert daher einige Standard-Appliances, wie z.B. Bedingung/Ereignis-Regeln, Zustandsübergangs-Regeln, Invarianten etc. Aber auch der Objekttyp "Appliance" kann vom BOCA-Programmierer verwendet werden, um zusätzliche Funktionalität als Ergänzung zu anderen Business Objects bereitzustellen.

```
entity small_customer {
  attribute float balance;
  apply Invariant small_balance {
    guard = (balance > 10000);
    schedule = DO_AFTER_COMMIT;
  };
};
```

Beispiel

Es wird eine Invariante für den Typ "small_customer" angewendet, die sicherstellt, daß der Kontostand >10.000 ist. Diese Regel wird immer angewendet, wenn ein Commit ausgelöst wurde.

Ein anderes Beispiel für die Verwendung von Appliances könnte die Auswahl eines Zahlungsverfahrens sein. Dabei stellt die Appliance sicher, daß für Käufer und Verkäufer nur ein Verfahren aktiviert wird, für das beide über die nötige Software verfügen.

Arten von Business Objects

Business Objects treten auf als *Entitäten* und *Prozesse*:

- Entitäten entsprechen dabei dem Entitätsbegriff des E/R-Modells. "Entity" dient dabei eine gemeinsame Basisklasse, von der Klassen wie "Kunde" oder "Projekt" abgeleitet sind. Entitäten definieren Schnittstellen von Objekten und kapseln ihr Verhalten.
- Prozesse sind einem anderen Business Object angefügt und sind selbst als Komponente realisiert (d.h. sie können andere Prozesse beinhalten). Prozesse unterscheiden sich von Business Objects dadurch, daß sie als Subklasse von "Process" definiert sind und die Aktivität eines anderen Business Object repräsentieren. Sie können diesem Objekt zusätzliche Features (also Attribute, Beziehungen, Regeln etc.) hinzufügen.

```
entity Truck {
  // Other truck stuff...
  process MoveTruck {
    [readonly]
    relationship the_truck References Truck;
    relationship move_to References place;
    state_set moving {ready_to_move, moving, moved, move_aborted};
  };
};
```

Beispiel: Prozess-Objekt eines Business Object "Truck"

Im Gegensatz zu Methoden wurde das Konzept des Prozesses zusätzlich gewählt, da ein Prozess im Sinne der BOCA-Definition eher geeignet ist, Entwicklungen mit langer Lebensdauer zu repräsentieren, den entsprechenden abstrakten Zustand dabei besser zu kapseln und – als Business Object – selbst Beziehungen zu anderen Objekten zu pflegen.

Business-Events sind – ähnlich Prozessen – abstrakte Ereignisse, die auf organisatorischer Ebene in oder zwischen BSDs auftreten. Wichtig ist hierbei, daß Business-Events aufgrund ihrer Eigenschaft Business Object persistent sein und wegen ihrer eindeutigen ID persistent verwaltet werden können.

Mit Hilfe der dargestellten Bausteine kann ein Anwendungsentwickler Objektkonfigurationen entwickeln, die im verteilten System die Aufbau- und Ablauforganisation eines Unternehmens widerspiegeln und die durch flexible Konfigurationsmechanismen die Anpassung an neue Anforderungen erleichtern können. Ohne die Möglichkeit, diese Konfiguration abstrakt zu modellieren, ist noch keine ausreichende Rationalisierung des Anpassungsprozesses erreicht. Aus diesem Grunde wurde das *BOCA-Metamodell* definiert, daß Spezifikation Beschreibung von Business-Object-Konfigurationen dient. Objekte des Metamodells existieren im Designwerkzeug des Modellierers und lassen sich entweder in Form von Meta-Objekten oder in textueller Form austauschen. Als Pendant zur IDL wurde die Component Definition Language als Austauschformat und Spezifikationsprache für Business Objects definiert. Dabei ist eine isomorphe Abbildung zwischen Objekten des Metamodells und CDL möglich, d.h. Metamodell und CDL sind lediglich zwei unterschiedliche Repräsentationsformen einer Spezifikation von Business-Objekt-Konfiguration. Mit der Hilfe von CDL können die Bausteine der BOF in einen syntaktisch und semantisch korrekten Zusammenhang gebracht werden.

Die Component Definition Language

CDL ist eine erweiterbare, deklarative Spezifikationsprache, die zur Beschreibung von Objektkonfigurationen im Unternehmen eingesetzt werden kann. Eine CDL-Spezifikation definiert dabei folgendes:

- Schnittstellen von Business Objects
- Strukturelle Beziehungen zwischen Business Objects
- Das kollektive Verhalten von Business Objects

CDL ist dabei eine textuelle Repräsentation des Metamodells für Business Objekte. Anwendungsprogramme werden nicht in CDL programmiert, daß CDL nur Schnittstellen, Beziehungen und Verhalten spezifiziert. Jedoch kann CDL in gängige Programmiersprachen transformiert werden, so daß ein Gerüst zum Füllen mit der eigentlichen Anwendungsfunktionalität generiert werden kann. Bei der Standardisierung der CDL wurden verschiedene bereits existierende Konzepte anderer Sprachen übernommen:

- Die CDL-Grammatik ist eine Obermenge von *IDL*. Sie ist erweitert um die oben genannten Konzepte, um semantische Zusammenhänge spezifizieren zu können.
- CDL wurde in Anlehnung an die *Object Definition Language* (ODL) der ODMG (Object Database Management Group) entwickelt, um z.B. die Anpassung von OML-Werkzeugen zu erleichtern.
- Die Syntax zur Definition von Ausdrücken ist an *Java* angelehnt.
- Schließlich floß OMG's *OCL* (Object Constraint Language) zur Spezifikation von Bedingungen und Anfrageausdrücken ein.

Die BOCA-Architektur sieht darüber hinaus die Möglichkeit vor, *UML-Modelle* abzubilden in CDL-Spezifikationen. Da nicht alle CDL-Konzepte in UML modellierbar sind, wird das Resultat immer nur einer Untermenge der CDL-Grammatik entsprechen; damit sind Ergänzungen und Verfeinerungen immer durch ein zusätzliches CDL-Werkzeug erforderlich. Allerdings hilft diese Integration mit UML, bereits genutzte Modellierungswerkzeuge wiederzuverwenden.

Am Output-Ende der "Spezifikationspipeline" erfolgt die Abbildung nach IDL. Dabei werden unterschiedliche Schnittstellendefinitionen generiert, um die Mächtigkeit von CDL durch entsprechende Standard-Methoden in IDL zu repräsentieren. Im folgenden Beispiel ist ein mehrwertiges Attribut *Attr2* definiert, das somit eine Liste von Integers umfaßt. Um diese Semantik in IDL repräsentieren zu können, wurde u.a. eine Schnittstellendefinition für *Attr2Iterator* generiert, mit deren Hilfe ein Client des Business Objects die Werte von *Attr2* auslesen kann.

Das dem Beispiel zugrundeliegende Werkzeug ist der CDL-Compiler von Data Acces [XXX], der neben der

IDL-Spezifikation zusätzlich noch Java-Code generiert. Verwendet man im nächsten Schritt dann einen IDL-nach-Java-Generator, lassen sich die generierten Methodenaufrufe (z.B. des IDL-Interface "Foo") an die generierten Schablonen der Java-Klasse "FooImpl" binden. Dabei wird ein default-Verhalten in den Java-Code generiert, das ein Testen des Codes erlaubt. In der Praxis hat der Modellierer jedoch darauf zu achten, daß der generierte Code konform ist zu existierenden Anwendungsklassen im Unternehmen. Gleiches gilt für jede andere Programmiersprache, die unterstützt werden soll.

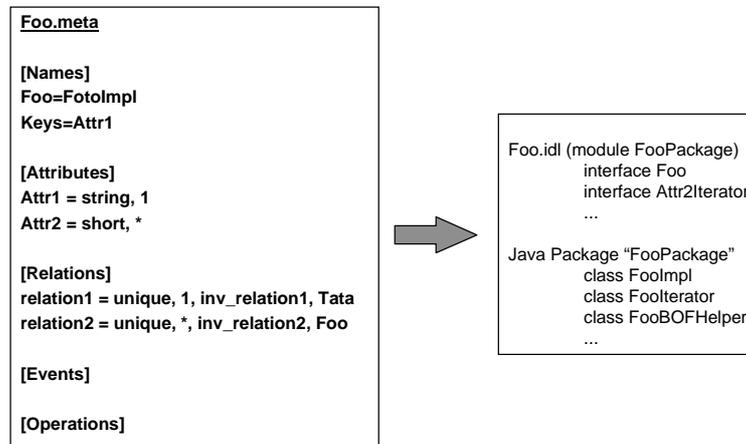


Abb. 45: Generieren von IDL-Code aus CDL-Code

Mit Hilfe der bisher beschriebenen Komponenten besteht nun die Möglichkeit, Konfigurationen von Business Objects zu modellieren (UML), dieses Modell im Sinne der BOCA um zusätzliche Elemente zu verfeinern (Regeln, Appliances etc.) und dies entweder syntaktisch in Form einer CDL-Spezifikation oder "im Hauptspeicher" in Form von Metamodell-Objekten zu spezifizieren. Anhand dieser Spezifikation wird anschließend zunächst eine IDL-Spezifikation generiert und anschließend (oder auch direkt) ein Programmgerüst der Zielsprache. Dieser gesamte Prozeß der Softwareentwicklung ist in folgender Graphik beschrieben:

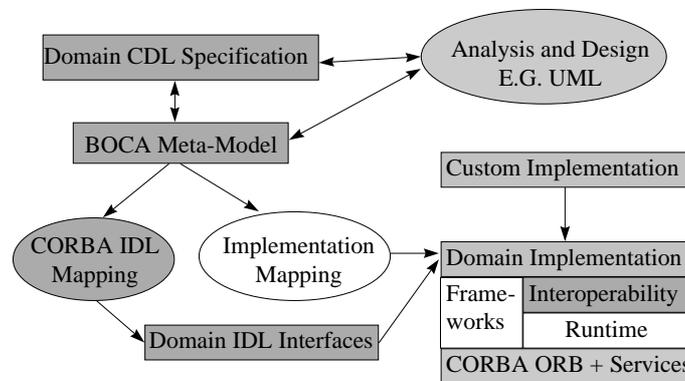


Abb. 46: Der Spezifikationsprozeß vom UML bis zum lauffähigen Code

Common Business Objects (CBO)

In der Hierarchie von Abstraktionsebenen der BOCA-Architektur treten erstmalig mit den Common Business Objects solche Objekte auf, die nicht der Verwaltung dienen, sondern anwendungsabhängig sind. Jedoch nur abhängig in dem Sinne, daß sie für die einen Anwendungen genutzt werden und für andere nicht. Sie sind jedoch nicht speziell zu entwickeln für eine konkrete Anwendung, z.B. die Lagerverwaltung. Stattdessen stehen Common Business Objects als Grundstock einer BOCA-Umgebung zur Verfügung – genauso wie bei CORBA Services davon ausgegangen wird, daß sie jedem ORB zur Verfügung stehen.

Beispiele für CBOs sind Währungstabellen, Konten usw. Eine Schwierigkeit ist in diesem Bereich, abzugrenzen, welche Business Objects eher noch als CBO aufzufassen und welche bereits so anwendungsspezifisch sind, daß sie aus der Menge der Standardobjekte herauszuhalten sind.

Die unter der OMG vereinten Unternehmen befinden sich auf der Ebene der CBOs in dem Kampf, einerseits

möglichst eigene Standardobjekte als CBOs vorzuschlagen und gleichzeitig die Vorschläge anderer Teilnehmer zurückzudrängen.

Wenn einmal Milch und Honig fließen...

Wenn auch die Tinte des BOCA-Standarddokumentes noch nicht getrocknet ist, soll an dieser Stelle kurz skizziert werden, welches Potential für den Business-to-Business-Commerce besteht, falls ein derartig mächtiges Framework einmal auf jedem Desktop bzw. Server installiert wäre.

Das Beispiel des virtuellen Unternehmens aus Kapitel XXX modellierte einen Publikationsagenten, der als 1-Personen-Unternehmen die Koordination von Zuliefererleistungen durchführte. Eine Umsetzung dieses Beispiels nach BOCA-Art könnte etwa folgendermaßen aussehen:

Mit Hilfe eines UML-Werkzeugs definiert der Agent Geschäftspartner, interne Objekte, Prozeßobjekte und allgemeine Bedingungen und Regeln für den Publikationsprozeß. Dabei werden auch zur Modellierung von Objekten fremder BSDs Spezifikationen für CBOs verwendet, da davon ausgegangen wird, daß in den dortigen Geschäftsbereichen "Druck", "Layout", "Autor" etc. standardisierte Objekttypen eingesetzt werden. Im Kern dieser Modellierung befindet sich der Geschäftsprozeß zur Publikation, der unterschiedliche interne und externe Objekte involviert. Einige dieser Objekte bestehen bereits, andere sind für jeden einzelnen Prozeß zu instanzieren.

Am Ende dieses Spezifikationsprozesses steht eine CDL-Datei (bzw. ein Modell) zur Verfügung. Mit einem neuen Publikationsauftrag des Autors wird dieses Modell instanziiert, d.h. es werden u.a.:

- ein neues Prozeßobjekt erzeugt,
- Verbindungen aufgebaut zu den Geschäftspartnern,
- Bedingungen und Regeln für den Prozeß und die beteiligten Objekte angepaßt.

Dabei ist für die Verbindungen festzulegen, welche Objektreferenzen auf Adapter fremder BSDs zu verwenden sind. Im Bereich der Regeln sind beispielsweise Lieferfristen und Preise anzupassen. Das auf diese Weise festgelegte Framework umfaßt somit nicht nur die Statik der Business Objects und ihrer Beziehungen, sondern auch die Dynamik der Auftragsabwicklung. D.h. der Publikationsprozess ist so vollständig beschrieben, daß ein Großteil der Aspekte, die üblicherweise durch einen Vertrag fixiert werden, bereits durch die Konfiguration festgelegt ist. Genau an dieser Stelle setzt Abschnitt XXX auf, bei dem wir mit dem Electronic Contracting noch einen Schritt weiter gehen: Dort wird vollständig auf den herkömmlichen Vertrag verzichtet – stattdessen wird die Objektkonfiguration um die juristische Bedeutung des Vertrages erweitert.

Zusammenfassung und Bewertung

Von allen Business-Object-Architekturen, die präsentiert werden, ist die BOCA die weitaus anspruchsvollste. Dabei ist ihre konzeptionelle Breite so groß, daß hier nur ein kleiner Ausschnitt behandelt werden konnte. Als Ergebnis der üblichen OMG-Standardisierungsprozeduren stellt die BOCA bisher die einzige als Standard verabschiedete Architektur dar. Alle anderen sind mehrere oder weniger proprietäre Entwicklungen. Der Nachteil dieser Komplexität liegt in ihrer Implementierbarkeit: Auch wenn es ansatzweise Werkzeuge wie den CDL/IDL/Java-Generator von Data Access gibt, stehen heute noch keine BOCA-konformen Werkzeuge oder gar Objekt-Frameworks zur Verfügung. Denkbar ist jedoch durchaus ein Wrapping existierender Produkte wie SAP oder San Francisco, so daß mit der BOCA zumindest eine Vereinheitlichung der unternehmensübergreifenden Kooperation erreicht werden kann.

Im Gegensatz zu den zuvor erläuterten Java Beans liegt die Qualität von BOCA in der Abstraktion von einer softwaretechnischen Sicht: Während bei Java Beans ein flexibler Integrationsmechanismus für Softwarekomponenten genutzt werden kann, um auch auf Module fremder BSDs zuzugreifen, ist die Sichtweise bei der BOCA umgekehrt. Hier steht die Modellierung von Geschäftsprozessen und -objekten im Vordergrund. Erst zweitrangig ist die Implementierung im Sinne der Programmiersprache und der konkreten Abbildung auf die technologische Infrastruktur.

Der Mangel an einem umfassenden CBO-Standard (jedenfalls auf absehbare Zeit) verhindert trotz allem, das wichtigste Problem zu lösen, das auch bei Java Beans bereits geschildert wurde: Ohne ein einheitliches Vokabular, d.h. ohne Standardisierung der Syntax *und* Semantik von Beans oder CBOs, besteht keine Chance, ein Drag'n'Drop zu unterstützen, welches erst die Ad-hoc-Integration von BSDs interessant macht.

Im wesentlichen gibt es nur zwei Möglichkeiten, diese semantische Kohärenz für eine domänenübergreifende

Integration zu erzielen: entweder ein proprietäres Produkt setzt sich durch oder Anwender sind in der Lage, selbst einen einheitlichen Standard zu definieren. Für beide Ansätze gibt es Beispiele mit unterschiedlichen Vor- und Nachteilen:

EDI ist das wenig erfolgreiche Ergebnis einer einvernehmlichen Standardisierung von Geschäftskommunikation. Es beschränkt sich lediglich auf die Spezifikation von Syntax und Semantik der Nachrichten und vernachlässigt dabei vollständig die Geschäftslogik.

Beispiele für den proprietären Ansatz sind SAP und IBM's San Francisco Project. Dabei hat SAP rechtzeitig Schlüsselanwendungen mit proprietären Modulen besetzen können, so daß aufgrund der gegebenen Netzwerkeconomie für jeden später Eintretenden die Entscheidung pro SAP umso leichter fällt, da bereits eine zunehmend wachsende Anzahl Geschäftspartner das Produkt einsetzt. Ähnliche, jedoch weniger erfolgreiche Produkte stehen ebenfalls von Baan, Oracle, Data Access oder IBM zur Verfügung. Im folgenden sollen zwei dieser Produkte aus der Perspektive der Business Objects beleuchtet werden: zum einen SAP wegen seiner Marktdurchdringung und zum anderen IBM's San Francisco wegen seiner relativ modernen Architektur.

7.3.4 Das San Francisco-Framework von IBM

San Francisco ist ein Produkt von IBM, dessen Entwicklung im Jahre 1996 zunächst in C++ begann, jedoch nach dem Siegeszug Javas rasch in dieser Programmiersprache fortgesetzt wurde. San Francisco ist ein Framework für Anwendungsobjekte, wie es bereits bei der BOCA-Architektur vorgestellt wurde. Jedoch kann sich IBM als Entwickler eines proprietären Produktes den Luxus leisten, das Framework komplett nach Java zu optimieren, so daß CORBA-spezifische Techniken und Overheads vermieden werden können.

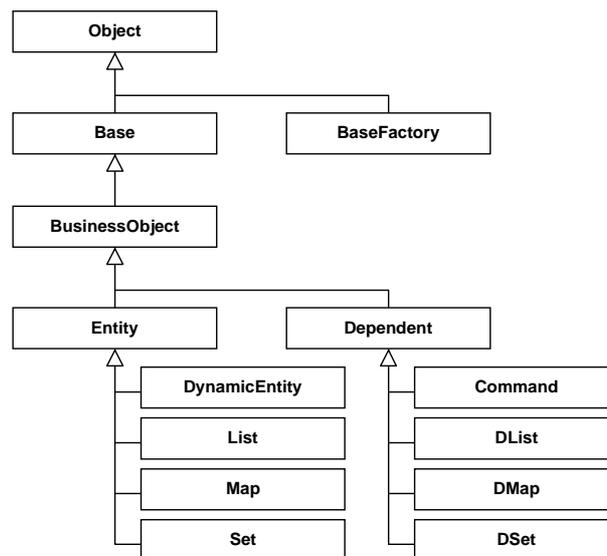


Abb. 47: Klassenhierarchie der San Francisco Foundation Classes

So wie wir Java Beans als Entwurfsmuster für Anwendungsklassen, die sich "Bean" nennen dürfen, kennengelernt haben, gibt auch das San Francisco-Framework ein gewisses Muster vor, dessen Anwendungen zu befolgen sind. Abb. XXX veranschaulicht die beteiligten Java-Klassen, die dem Framework der BOCA recht nahe kommen. Dies nicht ohne Grund, denn IBM war maßgeblich an der BOCA-Standardisierung beteiligt, verfolgte jedoch das Ziel, die San Francisco-Architektur vollständig als BOCA-Vorschlag einzubringen, um damit einen Wettbewerbsvorteil zu erzielen. Letztlich wurde BOCA ein Kompromiß, der maßgeblich auch auf die Vorstellungen anderer Beteiligter zurückzuführen war. Daher die Unterschiede zwischen BOCA und San Francisco.

Ebenfalls der BOCA ähnlich, setzen auf die Ebene der Basisklassen des San-Francisco Foundation-Layers CBOs auf. Diese sind vom Hersteller vorgefertigte, anwendungsneutrale Klassen, die für spezifische Zwecke wiederverwendet werden können. Sie liegen – ähnlich den CORBA Services bei der OMA – bei jeder San-Francisco-Installation vor. Die nächst-höhere Ebene setzt sich zusammen aus sog. "Core Business Processes" – Objekten, die grundlegende Geschäftsprozesse und dafür erforderliche Module realisieren. Diese Frameworks können wiederum horizontal (Workflow, Buchhaltung) oder vertikal sein (Bankwesen, Produktion). Schließlich wird diese Hierarchie durch Eigenentwicklungen des Anwenders abgeschlossen. Abb. XXX zeigt die Gesamtarchitektur des Frameworks:

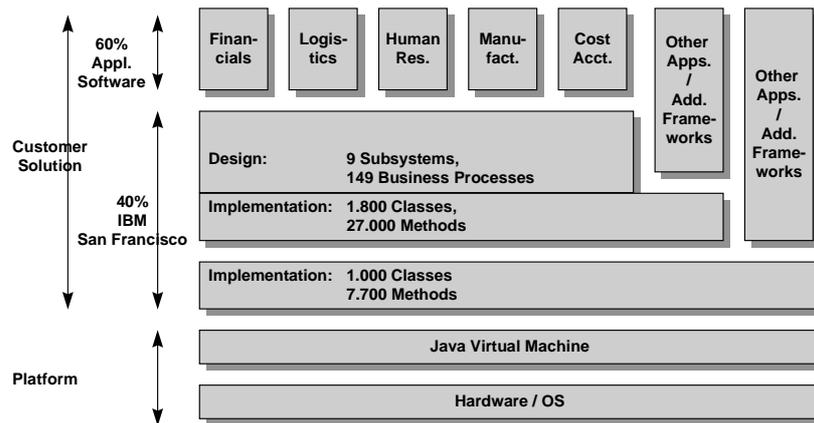


Abb. 48: Die Architektur des San-Francisco-Frameworks

Programmiertechnisch liegt Java Beans der San-Francisco-Entwicklung zugrunde. Dies gilt grundsätzlich für alle Bestandteile des Frameworks. Da die anwendungsnahen Objekte jedoch in der Regel eine intensive Datenbanknutzung erfordern, war es konsequent, daß auch EJBs zur Realisierung von Business Objects (insbesondere der persistenten Entities) herangezogen wurden. Dabei ergänzen sich EJB und SF recht gut: während EJB ein Entwurfsmuster für die persistente Verwaltung von Beans liefert, liegt IBM's Mitgift in einer Ansammlung vorgefertigter Anwendungsmodule.

Zusammenfassung

Mit San Francisco liegt erstmalig ein Produkt vor, welches als komponentenbasiertes Framework für Geschäftsanwendungen bezeichnet werden kann. Unter der Annahme, daß ein Großteil der Anwender eine solche Infrastruktur einsetzen, kann Hoffnung reifen, daß sich die Betriebs- und Anpassungskosten soweit reduzieren lassen, daß auch unternehmensübergreifende Kooperation realisierbar wird und wir der Vision eines virtuellen Unternehmens etwas näher kommen.

Zwei schmerzliche Wehmutstropfen sind jedoch zu verkraften: erstens wird San Francisco noch zu sehr durch die langsame Ausführungsgeschwindigkeit von Java gebremst. Hier besteht noch Hoffnung auf Besserung in den nächsten Jahren.

Das zweite Problem liegt im Wettbewerber SAP. Während sich IBM, Oracle, Baan oder Data Access noch jeden Kunden erobern müssen, hat die Marktmacht von SAP ein Ausmaß erreicht, das einem Anwender neben dem lokalen Nutzen der SAP-Einführung zusätzlich fast eine Garantie auf Interoperabilität mit Geschäftspartnern zusichert. Angesichts dieser Situation stellt sich die Frage, ob der technologische Mehrwert einer modernen Architektur vom Anwender wahrgenommen werden kann. Aus diesem Grunde folgt eine kurze Übersicht bez. des Systems R/3 und die Nutzung von Business Objects in diesem Zusammenhang.

7.3.5 Zusammenfassung

XXX Machen!

XXX Bis hier Orthographie korrigiert

7.4 Workflow-Management zwischen Unternehmen

Workflow-Management-Systeme (WFMS) werden eingesetzt, um die richtige Ressource mit der richtigen Aufgabe zum richtigen Zeitpunkt zu versorgen. Diese Koordinationsaufgabe ist üblicherweise auf einen Dienst ausgelagert, der andere Teilnehmer hinsichtlich ihrer Aktivitäten steuert. Als traditionelle Beispiele für Geschäftsprozesse, die sich mit Hilfe von WFMS optimieren lassen, sind Dienstreiseanträge zu nennen oder auch Schadensmeldungen bei Versicherungen. Diese Prozesse sind wohlstrukturiert und wiederholen sich so oft, daß sehr viel Aufwand in die Bereitstellung der Workflow-Unterstützung investiert werden kann.

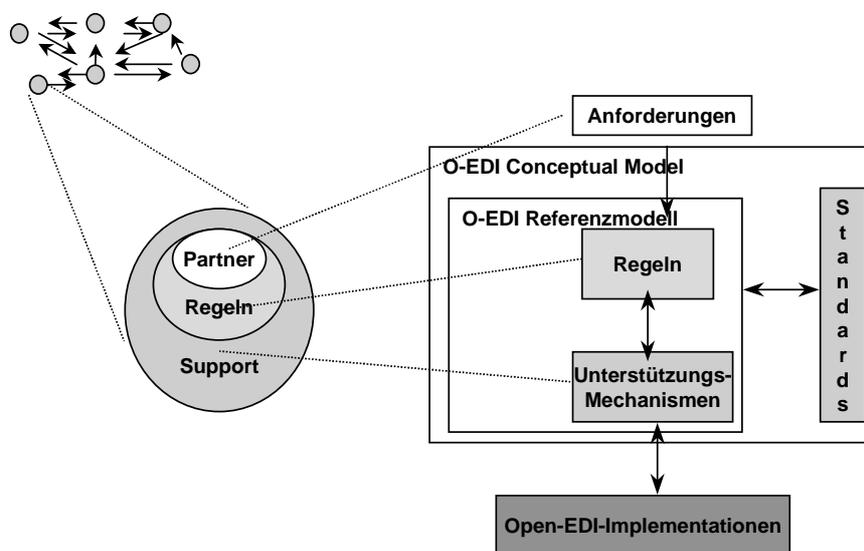
Ganz anders verhält es sich bei Prozessen, die sich über Unternehmensgrenzen hinweg erstrecken.

7.4.1 Allgemein

Grundlegende Einführung in WFMS

7.4.2 Beispiele

7.4.3 Open EDI?



7.4.4 Open Trading Protocol?

7.5 Elektronische Verträge

Wann immer wir im Internet ein Buch kaufen, ein Ticket bei einer Auktion ersteigern oder mit Lieferanten Bestellmodi vereinbart werden, dieser Handlung liegt immer ein impliziter oder expliziter *Kaufvertrag* zugrunde. Heute bestehen jedoch nur begrenzte Möglichkeiten, vertraglich vereinbarte Leistungen einzufordern, wenn die erforderliche Sicherheitsinfrastruktur fehlt. An wen kann man sich wenden, wenn das gelieferte Buch das falsche ist und der Händler abstreitet, daß jemals ein anderes bestellt wurde? An wen kann sich umgekehrt der Händler wenden, wenn vereinbart wurde, daß eine Zahlung per Rechnung nicht durchgeführt wurde und keine Unterschrift des Kunden vorliegt? In dieser Situation handelt es sich um Willenserklärungen der beteiligten Parteien über größere Distanzen und mittelbar über das Internet. Keiner kann also ohne weiteres die Authentizität des Gegenüber feststellen und dessen Willenserklärung anschließend einfordern. Wir haben es folglich mit einem immateriellen Vertrag zu tun, bei dem noch nicht einmal Sicherheit über die Echtheit der Willenserklärung besteht.

Elektronische Verträge sollen hier Abhilfe schaffen. Dabei decken sie alles ab was auch durch Verträge in Schriftform geregelt werden kann: Kaufverträge, Gesellschafterverträge, Eheverträge etc. An dieser Stelle wollen wir uns mit solchen beschäftigen, die eher für den EC-Bereich relevant sind. Dies sind z.B. Kaufverträge, geschäftliche Vereinbarungen, Pflichtenhefte und rechtsverbindliche Projektpläne.

Elektronische Verträge liegen immer explizit vor, d.h., es existiert ein Dokument, aus dem die Parteien, der Vertragsgegenstand, Bedingungen und Vereinbarungen sowie die geleisteten Unterschriften hervorgehen. Dieses

Dokument steht nach Vertragsschluß allen beteiligten zur Verfügung, so daß Leistungsverpflichtungen nicht abgestritten werden können.

Ein solcher Mechanismus garantiert Authentizität und Nichtabstreitbarkeit. Viele Web-Applikationen könnten von dieser Technologie profitieren, wenn sie sinnvoll in die Middleware des Internet (Web-Browser und – Server) integriert ist. Beispielanwendungen sind Online-Banking, Reservierungsdienste, Shops, aber vor allem auch Extranet-Anwendungen.

Die Frage lautet nun, wie ein solcher Vertrag erreicht werden kann. Wie soll der Prozeß der Vereinbarung und das Leisten der Unterschrift realisiert werden. Schließlich stellt sich die Frage, ob in der Abwicklungsphase die Daten eines Vertrages wiederverwendet werden können, um zu kontrollieren, ob die Leistungen ohne Verzug erbracht werden. Diese und weitere Aufgaben zählen zum Bereich des Electronic Contracting und werden im folgenden Schritt für Schritt erläutert:

7.5.1 Vertragsformen

Verträge werden in unterschiedlicher Form geschlossen. Grundsätzlich besteht Vertragsfreiheit, d.h. für die meisten Rechtsgeschäfte des täglichen Lebens existieren keine Formvorschriften, wie ein Vertrag gestaltet ist, auf welchem Medium er niedergeschrieben wird, welche Punkte explizit zu regeln sind usw.

Unterschieden werden üblicherweise *schriftliche und mündliche Verträge*. Dabei steht bei schriftlichen Verträgen für alle Parteien ein Dokument zur Verfügung, aus dem erkennbar ist, daß die andere Partei sich zum Gegenstand bekennt. Ein mündlicher Vertrag ist bei alltäglichen Geschäften wie dem Einkauf im Supermarkt gegeben. Dazu muß noch nicht einmal das Kaufinteresse mündlich zum Ausdruck gebracht werden, wenn durch *konkludentes Handeln* signalisiert wird, daß ein Kauf beabsichtigt ist (das Ablegen der Ware auf dem Fließband der Kasse).

Personen und Vertretung

Die Anzahl der Parteien kann zwischen zwei und beliebig vielen variieren. Eine einzelne Person kann somit keinen Vertrag mit sich selbst schließen. Bei Gesellschafterverträgen oder Kooperationsvereinbarungen mehrerer Unternehmen kann die Liste der Parteien sehr umfangreich werden. Eine Partei ist dabei unmittelbar beteiligt oder durch eine oder mehrere andere vertreten. Parteien werden danach unterschieden, ob sie juristische oder natürliche Personen sind. Erstere sind beispielsweise GmbHs, Aktiengesellschaften oder eingetragene Vereine. Natürliche Personen können nur Menschen sein. Eine juristische Person muß immer durch mindestens eine natürliche vertreten werden. Dies ist etwa der Geschäftsführer einer GmbH, oder eine Person, die ausdrücklich zur Vertretung der juristischen Person autorisiert ist. Die Autorisierungsbeziehung kann sich beliebig fortsetzen, d.h., der Geschäftsführer einer GmbH kann im Namen einer anderen GmbH zeichnen, die durch die erste vertreten wird. Oder ein Geschäftsführer kann eine zweite natürliche Person bevollmächtigen, um ihn selbst im Hinblick auf die Firma zu vertreten.

Die Vertretungsvollmacht kann qualifiziert erteilt werden. Hier handelt es sich üblicherweise um Einschränkungen im Transaktionswert („Aufträge bis 100.000 Euro darf Herr Schulze erteilen“) oder mehrere Personen werden nur im Kollektiv bevollmächtigt (Nur Herr Schulze und Frau Schröder zusammen dürfen Aufträge bis 200.000,- Euro erteilen). Die Bevollmächtigung kann schließlich zu einem komplexen logischen Ausdruck führen, der die Menge der bevollmächtigten Personenkonstellationen spezifiziert („Zwei Mitarbeiter aus der Abteilung Einkauf in Verbindung mit Herr Schröder sowie einem Vortandsmitglied...“).

Aufgrund gesetzlicher Auflagen sind Stellvertreterregelungen bei publikationspflichtigen Gesellschaften öffentlich bekanntzugeben. Diese Information ist im Handelsregister einzusehen und wird in Auszügen in einigen Tageszeitungen abgedruckt. Das Handelsregister fungiert dabei als Zertifizierungsstelle, die Attributzertifikate verwaltet. Im Gegensatz zum Trust-Center für öffentliche Schlüssel erteilt sie die Vollmachtenzertifikate jedoch nicht selbst, sondern sichert nur deren Authentizität zu. Vollmachtenzertifikate werden hingegen von den Unternehmen dezentral erteilt. Somit besteht ein wesentlicher qualitativer und organisatorischer Unterschied zum Trust-Center. Im Hinblick auf sein „Dokumentenmodell“ kann jedoch das klassische X.500-Zertifikat in erweiterter Form übernommen werden. Hier mangelt es jedoch noch an der erforderlichen Standardisierung von Syntax und Semantik des verwendeten Vokabulars (ganz ähnlich dem EDI-Problem...).

Praktiker und Juristen, die insbesondere im Außenhandel tätig sind, weisen häufig darauf hin, daß ein erheblicher Teil aller Rechtsstreitigkeiten auf dem Abstreiten von Willenserklärungen beruht, die nicht autorisierte Personen im Namen des Unternehmens lieferten. Eine Vertrauensinfrastruktur würde somit Rechtsunsicherheit vermeiden helfen, die mit klassischen Methoden (Auskunftsdienste, Handelsregister) nur sehr ineffizient reduziert werden

kann. Bereits hier zeichnet sich ab, in welchem Volumen Transaktionskosten einer „promiskuitiven“ Netzökonomie vermieden werden können.

Komplexe Vertragswerke

Verträge können als Bindeglied zwischen mehreren Parteien eingesetzt werden, wenn ein komplexer Workflow zwischen diesen festzulegen ist. Damit lassen sich innerhalb eines Konsortiums kreisförmige Lieferbeziehungen definieren oder auch Parteien zu Interessengemeinschaften bündeln:

Die Publikation eines Buches kann auf einem Vertragswerk basieren, das zwischen einem Publikationsagenten (vgl. den Abschnitt über virtuelle Unternehmen XXX), seinem Auftraggeber (dem Autor) sowie einer Gruppe unterschiedlicher Dienstleister geschlossen wird. Dabei können alle Beteiligten am gleichen Vertrag mitwirken oder auch an mehreren Einzelverträgen. Im ersten Fall besteht für alle Beteiligten Transparenz – auch bez. der Konditionen anderer Teilnehmer. Dies ist nicht immer im Interesse des Koordinators, der dem Autor vielleicht seine tatsächlichen Partner verbergen will. Abb. XXX verdeutlicht hierbei die zweite Variante.

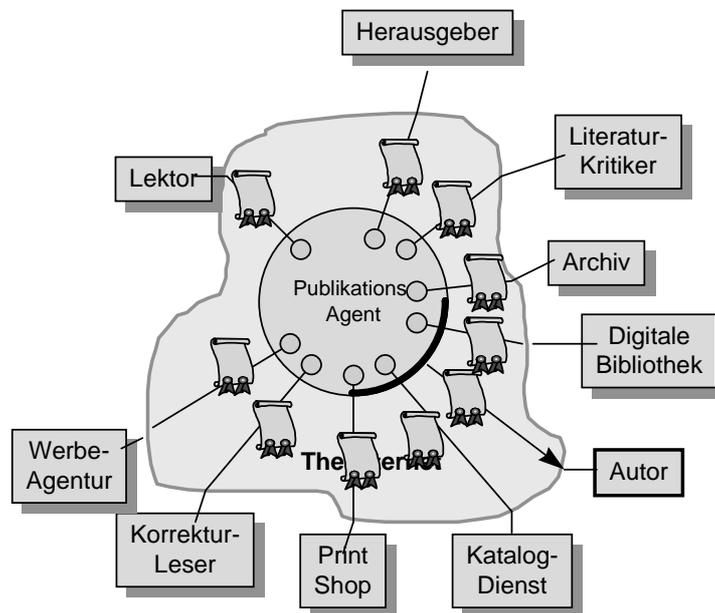


Abb. XXX: Vertragsbeziehungen des Publikationsagenten

Die Bedeutung eines solchen Vertragswerkes liegt in einer Unterscheidung der Sichtbarkeits- und Vertrauensbeziehungen einerseits von der Atomarität des Gesamtwerkes andererseits: Die isolierte Beauftragung des Korrekturlesers macht genausowenig Sinn wie die des Print-Shops, wenn keine Auftragsbeziehung mit dem Autor vorliegt. Auch die Unterzeichnung des Autorenvertrags erfordert häufig eine Vorallokation der anderen Dienstleistungen, um den Produktionsprozess abzuwickeln. Folglich kann das Vertragswerk als eine Menge von Einzelaufgaben aufgefaßt werden deren gemeinsamer Nenner in einem transaktionalen Vertragsschluß liegt. Nur wenn alle Teilverträge geschlossen wurden, tritt das Vertragswerk in Kraft. Dieser Zusammenhang läßt sich durch entsprechende Rahmenverträge zwischen dem Koordinator und den Vertragsparteien herstellen, so daß der Electronic Contracting Service als allen Beteiligten zusichern kann, daß ein Auftrag abgewickelt wird, wenn alle Teilverträge geschlossen sind. Dies gibt den Parteien eine gewisse Planungssicherheit und reduziert damit das unternehmerische Wagnis.

Eine andere Form multilateraler Verträge fördert den Zusammenschluß homogener Vertragsparteien. Als Beispiel stelle man sich das Broker-Szenario aus Abschnitt XXX vor: 200 Privatpersonen schließen sich zu einer Einkaufsgemeinschaft zusammen, um jeweils einen Mercedes SLK zu kaufen. Sie erfüllen gemeinsam die Rolle der Käuferpartei und legen einen Vertragsentwurf fest, der einen Rabatt von 25% vorsieht. Jeder Teilnehmer verpflichtet sich, beim Zustandekommen eines Vertrages das spezifizizierte Fahrzeug zu kaufen. Wenn sich 200 Interessenten gefunden haben, wird der Hersteller (als 201. Partei) aufgefordert, dem Angebot zuzustimmen. Evtl. kann sich eine Verhandlung um Konditionen und Preise anschließen, die evtl. eine Veränderung des Einkaufskonsortiums bewirkt. Am Ende schließen jedoch alle noch beteiligten Parteien einen Vertrag bei 17% Rabatt. Dem Hersteller bieten solche Verträge ebenfalls Planungssicherheit sowie die Möglichkeit, Kosten der Ver-

triebskette zu vermeiden.

Weitere Vorteile elektronischer Verträge

Die Verwendung elektronischer Verträge hilft des Weiteren, die Ausarbeitung des Dokuments zu strukturieren. Dabei kann ein Autorensystem verwendet werden, das es den Parteien erlaubt, gemeinsam den Vertrag zu editieren. Da dieser aufgrund seiner Natur ein strukturiertes Dokument ist, läßt sich das Editieren problemlos koordinieren. Zudem hilft ein entsprechender Online-Dienst, Redundanzen und Inkonsistenzen zu vermeiden, die auftreten, wenn Verträge zwischen mehreren Parteien z.B. als Word-Dokument zirkulieren. Bis zu einem gewissen Grade läßt sich auch der Vertragsinhalt automatisch validieren. Geht man von einem vorgegebenen Datenmodell (oder Dokumentenmodell) für Verträge aus, kann die Integrität des Vertrages festgestellt werden. Ist beispielsweise eine Partei beteiligt die für keine der festgelegten Leistungen als Erbringer oder Empfänger definiert wurde, ist das System in der Lage, solche Situationen zu erkennen. Auf juristisch inkonsistente Zustände kann das System ebenso hinweisen wie auf In-sich-Geschäfte oder ökonomisch unsinnige Workflows.

Letztlich hilft ein Electronic-Contracting-System durch diese Maßnahmen Transaktionskosten zu senken durch die schnellere Ausarbeitung und Unterzeichnung eines Vertrages. Gerade unter der Anforderung an Unternehmen, sich schnell mit anderen zusammenschließen zu können, ist diese Eigenschaft von existenzieller Bedeutung. Nur auf elektronischem Wege wird in Zukunft ein Unternehmen konkurrenzfähig bleiben.

7.5.2 Transaktionsphasen

Entlang der Transaktionsphasen Information—Verhandlung—Abwicklung läßt sich auch der elektronische Vertrag in seinem Werdegang vom halbfertigen Formular bis hin zur notarierten Handlungsanweisung verfolgen. Diese drei Phasen sowie ihre jeweiligen Übergänge lassen sich anhand des Publikationsbeispiels folgendermaßen charakterisieren:

Informationphase

Es wird angenommen, daß die Initiative vom Autor ausgeht, welcher einen Vertragsentwurf benutzt, um einen geeigneten Publikationsagenten zu ermitteln. Dabei wird die Rolle des Agenten spezifiziert durch eine Mindestforderung bez. des Autorenhonorars, eine Nennung verschiedener Schlagworte, welche das Fachgebiet der Publikation kennzeichnen, sowie durch weitere Attribute, welche z.B. die Behandlung von Urheber- und Verwertungsrechten betreffen.

Der Broker liefert dem Autor eine Liste von Publikationsagenten, von denen der günstigste ausgewählt wird. Damit steht eine Vertragsschablone bereit, bei der die beiden Rollen „Autor“ und „Publikationsagent“ instanziiert sind. Für den Auftraggeber nicht sichtbar, hat der Publikationsagent selbst weitere Rollen (Druckerei, Korrekturleser, etc.) mit entsprechenden Anbietern besetzt, so daß dem Autor als Bestandteil des Vertrages schließlich ein Honorar angeboten werden kann, welches dem geforderten entspricht und dem Publikationsagenten eine geeignete „Handelsspanne“ zusichert.

Verhandlungsphase

Nun wird der Vertrag mehrmals zwischen Autor und Publikationsagent ausgetauscht, um Fristen, Zahlungsmodalitäten, etc. zu verhandeln. Diese waren bereits in der Vertragsschablone vordefiniert, müssen jedoch für den konkreten Vertragsfall noch angepaßt werden.

Die Verhandlung erfolgt dabei als Workflow, welcher innerhalb der jeweiligen Parteien ausgeführt wird. Der Transfer des Vertrages von einer Partei zur nächsten stellt eine Aktivität des Prozesses der sendenden, das Eintreffen des Vertrages beim Empfänger den Anstoß oder Wiederanlauf eines weiteren Prozesses dar.

Sobald bez. aller Aspekte Einigung erzielt wurde, unterschreiben beide Parteien den Vertrag mit ihrem privaten Schlüssel und fügen Unterschrift und Zertifikat dem Vertrag bei. Gleiches erfolgt zwischen dem Publikationsagenten und allen Subauftragnehmern. Diese untergeordneten Verträge müssen jedoch nicht synchron mit dem Vertrag des Autors abgeschlossen werden, da die verbindliche Zusage des Publikationsagenten gegenüber dem Autor nur die Bedingungen, jedoch nicht die Existenz bzw. Implementierung der Subaufträge offenlegt.

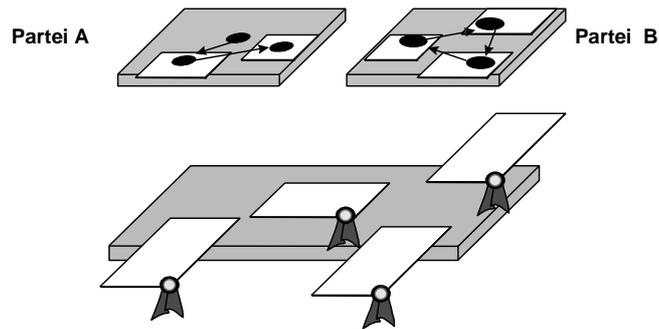


Abb. XXX: Vertragsbeziehungen zwischen Parteien

Abwicklungsphase

Anhand der definierten Fristen können alle Vertragspartner durch das Electronic-Contracting-System benachrichtigt werden, wann eine Aktivität zu erfolgen hat. Dies bedeutet im Anwendungsfall, daß z.B. für das Korrekturlesen ein Zeitrahmen von 14 Tagen vereinbart wird und daß diese Tätigkeit spätestens 3 Tage nach Eintreffen des Manuskripts vom Autor zu beginnen ist.

Nachdem das Korrekturlesen abgeschlossen wurde, ist das Dokument an den Autor zurückzusenden, für den eine Frist von 4 Wochen zur Überarbeitung des Dokuments vereinbart wurde. Schließlich hat der Publikationsagent das Dokument an die Druckerei weiterzuleiten.

Diese Bedingungen und Fristen werden vom Electronic-Contracting-System überwacht. Im Falle der Überschreitung werden die beteiligten Parteien informiert, so daß alle betreffenden Instanzen über den Zustand des Vorgangs benachrichtigt sind.

Eventuell kann ein Vertrag so abgeschlossen sein, daß gewisse Bestandteile auch nach seinem Abschluß noch modifiziert werden können. Dies kann beispielsweise der Fall sein, wenn Rahmenverträge zu einem späteren Zeitpunkt durch Anhänge oder Ergänzungen erweitert werden. Diese Situation kann beispielsweise im Anwendungsbeispiel auftreten, wenn der Publikationsagent vom Autor auch die Verwertungsrechte für eine Filmproduktion gegen ein zu verhandelndes Honorar erhält.

7.5.3 COSOMOS – Ein Internet-Dienst für das Electronic Contracting

COSMOS steht für Common Open Service Market fOr Small and medium enterprises. Es ist ein Industrieprojekt, an dem die folgenden Unternehmen beteiligt sind:

- *Ponton Hamburg* (Internet-Softwareunternehmen zur Realisierung von Client- und Serverkomponenten)
- *Universität Hamburg* (Arbeitsgruppe Verteilte Systeme am Fachbereich Informatik)
- *Oracle* (Datenbank und Middleware-Technologie),
- *Cefriel* (Spezialist für Internet-Security aus Mailand)
- *SIA* (Betreiber des italienischen Interbankennetzes und des SWIFT-Gateways)
- *INESC* (Portugisisches Informatik-Forschungsinstitut)
- *IMP* (Londoner Musikverlag als Testnutzer)

Die Universität Hamburg steuerte Teile der Architektur sowie der Softwareentwicklung bei. Dem aufmerksamen Leser dürfte nicht entgangen sein, daß dieses projekt mein persönliches geistiges Kind ist und daß seine Wurzeln auf meine Zeit an der Universität zurückgehen. Zum Zeitpunkt der Publikation dieses Buches dürfte es nicht mehr lange dauern bis zur Verfügbarkeit der Testinstallation auf dem Server www.ponton-hamburg.de. Wir bitten um regelmäßigen Check.

Nun jedoch Schluß mit der Schleichwerbung, wenden wir uns wieder der Technologie zu! Gemeinsame Grundlage der COSMOS-Architektur ist ein Objektmodell für elektronische Verträge, eben das *Vertragsmodell*. Es legt Komponenten, Beziehungen und Rollen für elektronische Verträge fest sowie Software-Schnittstellen zur Verhandlung, Unterzeichnung und Ausführung. COSMOS nimmt für sich in Anspruch, alle Transaktionsphasen ohne

Medienbruch zu unterstützen. Dabei greift das System auf einen Katalog zurück, der zur Registrierung von Vertragsangeboten verwendet wird. Broker dienen der Vermittlung der registrierten Angebote und liefern Vertragsvorschläge, die anschließend verhandelt werden können. Ein elektronischer Notar übernimmt die Koordination der Unterzeichnung, so daß Betrugsversuchen und möglichen Inkonsistenzen vorgebeugt wird. Diese Bestandteile werden im folgenden ausführlicher beschrieben. Informationen über aktuelle Entwicklungen werden über den Web-Server von Ponton Hamburg freigegeben.

7.5.4 Ein Objektmodell für elektronische Verträge

Die COSMOS-Architektur unterstützt alle Transaktionsphasen, daher ist die Nutzung eines einheitlichen Objektmodells über alle Phasen hinweg vorteilhaft. Aus Gründen der Übersichtlichkeit und des beschränkten Platzes wird im folgenden jedoch nur das Vertragsmodell skizziert. Eine ausführliche Behandlung aller Komponenten ist in [MGTM+98] zu finden. Die wesentlichen Merkmale dieses Objektmodells werden im *Vertragsmodell* zusammengefaßt. Es zielt darauf ab, nur jene Vertragsbestandteile zu formalisieren, die semantisch eindeutig abgrenzbar sind und damit eine effiziente Automatisierung erlauben. Abbildung 3 illustriert das entwickelte Objektmodell.

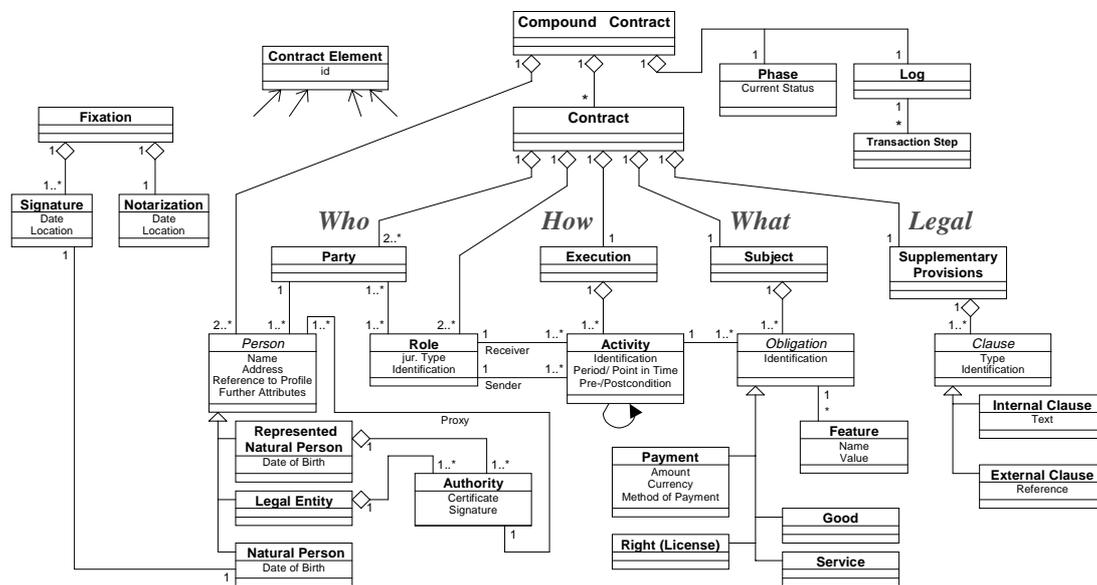


Abb. 49: Das COSMOS Vertragsmodell

Die Bestandteile des Vertragsmodells werden im folgenden nach ihren Schwerpunkten unterschieden:

Das Vertragswerk

- Ein *Vertragswerk* (engl. "compound contract") ist ein Verbund mehrerer Einzelverträge. Dabei können diese jeweils in sich abgeschlossen sein oder untereinander Querbeziehungen besitzen. Das Vertragswerk setzt sich zusammen aus Verträgen, einer Liste von Unterschriften, sowie Meta-Informationen zum Zustand des Vertragswerks.
- *Vertrag*. Ein Vertrag ist ein Objekt, welches sich aus einer Menge von *Klauseln* zusammensetzt und anwendungsspezifisch um zusätzliche Klauseln erweitert werden kann. Ein Vertrag liegt im juristischen Sinne erst vor, wenn alle *Parteien* diesen signiert haben. Ein Vertrag definiert immer mindestens zwei *Leistungen*, die jeweils von einer der Parteien erbracht werden.
- *Klausel*. Ein *Vertrag* besteht strukturell aus Klauseln. Diese sind im wesentlichen den folgenden Bereichen zuzuordnen: Identifikation der Parteien („Wer“), des Vertragsgegenstands („Was“), der Durchführung („Wie“) sowie weiteren Bedingungen.
- Auf der Ebene des Vertragswerks werden *Metainformationen* verwaltet, die sich auf einzelne Verträge bzw. das gesamte Vertragswerk beziehen. Diese umfassen *Unterschriften* und *Statusinformationen*.

- *Unterschriften* werden von den *Parteien* für einen *Vertrag* geleistet. Befinden sich mehrere Verträge im Vertragswerk, so hat jede Partei alle Verträge zu unterschreiben, an denen sie als Partei beteiligt ist.
- *Beglaubigung des Notars*. Der *Notar* hat die Unterschriften der Parteien zu validieren und mit seiner eigenen Unterschrift den Zusammenhang dieser Unterschriften mit den Verträgen zu beglaubigen.
- *Statusinformation*. Ein Vertrag kann sich in den Zuständen „Schablone“, „Vorschlag“, „Angebot“, „Agreed“, „Unterschrieben“, „In Ausführung“ befinden. Diese Information kann dem Vertragsobjekt über einen Methodenaufruf entnommen werden. Sie sollte sich aus der Zusammensetzung der Vertragsstruktur ableiten lassen, so daß keine explizite Repräsentation des Zustandes (als Attribut) erforderlich ist.

Parteien

- *Partei*. Organisatorisch wird ein *Vertrag* zwischen zwei oder mehreren Parteien geschlossen. Dabei qualifiziert der Begriff „Partei“ einen *Marktteilnehmer* als Vertragsteilnehmer. Er legt jedoch weder die *Rolle* fest, in der die Partei agiert, noch die Person(en), die sie repräsentiert.
- *Personen* treten (synonym für *Teilnehmer*) als Vertragsparteien auf. Dabei können Personen in mehrere Verträge involviert sein. Eine Person kann - gemäß dem Vertragsmodell - entweder eine juristische oder eine natürliche Person sein. In beiden Fällen sind hinreichend Informationen erforderlich zur Authentisierung der Person, zur Integration in Workflow-Prozesse sowie zur Spezifikation der individuellen Anforderungen an die COSMOS-Infrastruktur.
- *Rolle*. Eine *Partei* nimmt für einen individuellen *Vertrag* eine spezielle Rolle ein, z.B. „Verkäufer“, „Käufer“ oder „Finanzier“.

Vertragsgegenstand

- Der *Vertragsgegenstand* setzt sich aus mehreren *Leistungen* zusammen, welche die Parteien untereinander austauschen. Eine Leistung besitzt Qualitätsattribute, die sich von Vertrag zu Vertrag unterschiedlich zusammensetzen können. Eine Leistung (engl. "obligation") repräsentiert grundsätzlich die Übertragung eines Rechts. Dieses Recht kann das Eigentum an einer *Ware*, an *Geld*, einer *Dienstleistung* oder eine *Lizenz* sein. Eine Leistung besitzt immer einen (Leistungs-)Erbringer und einen (Leistungs-)Empfänger. Dabei sind in diesem Bereich auch Abhängigkeiten zwischen Leistungen festzulegen. Diese umfassen im Rahmen der *Durchführung* kausale und temporale Abhängigkeiten zwischen jeweils zwei Leistungen: Bedingungen, unter denen eine Leistung zu erbringen ist, Informationen, die zwischen zwei Leistungen transferiert werden, sowie Informationen, die als Parameter bzw. Resultat einer Leistung auftreten. Leistungen sind im einzelnen:
 - *Ware*: Hierbei wird anhand der *Leistungsattribute* eine Produktbeschreibung vorgenommen
 - *Dienstleistung*: Die QoS-Parameter eines Dienstes werden hier festgelegt. Ferner kann eine Dienstleistung online – d.h. durch einen Server - erbracht werden. Im Falle der Online-Dienstleistung ist dazu eine URL auf eine *Adapter-Bean* erforderlich, die als Proxy für Methodenaufrufe beim Dienstleister verwendet wird (s.u.).
 - *Lizenz*: Hierbei wird ein authentisiertes Datenobjekt vom Leistungserbringer an den -empfänger übermittelt.
 - *Geld*: Auch hier wird ein Datenobjekt übermittelt. Es kann sich um eine Zahlungsautorisierung oder um eine elektronische Münze handeln.

7.5.5 Die COSMOS-Architektur

Die COSMOS-Architektur zielt darauf ab, Transaktionskosten sowohl durch *Automatisierung* als auch durch *Integration* zu reduzieren. Dies betrifft vor allem folgende Softwarekomponenten (vgl. Abb. 2):

Softwarekomponenten der COSMOS-Architektur

- *Online-Kataloge*. Informationen über Marktteilnehmer können heute über Suchmaschinen oder „Gelbe-Seiten“-Dienste erlangt werden. Beiden Ansätze mangelt es jedoch an Selektivität auf der Basis einer geeig-

neten Menge von Qualitätsattributen. Diese würden Anbietern die Möglichkeit gewähren, nicht nur Teilnehmerinformation, sondern auch Angebote zu registrieren. Nachfragern würden die Attributlisten als Hilfsmittel dienen, um präzisere Anfragen zu formulieren.

- **Broker** arbeiten im Auftrag eines Teilnehmers, um ein Konsortium aus potentiellen Vertragspartnern zu formieren. Sie benötigen sowohl Zugang zum Online-Katalog als auch zu den QoS-Spezifikationen der Nachfrager. Richtlinien zur Auswahl und Navigationsschnittstellen unterstützen Anwender des Brokers in flexibler Form. Als Kernkomponente des Brokers dient ein Trader, wie er im Rahmen der ODP- bzw. CORBA-Standardisierung spezifiziert wurde [ISO97, MJML95, OMG96]. Im Gegensatz zum CORBA-Trader ist der Broker jedoch in der Lage, Angebote zu mehr als einer Spezifikation (der „Import“-Anfrage des Traders) zu liefern. Resultat des Brokers ist dabei ein *Vertragsvorschlag*, welcher zu jeder vertraglich definierten Rolle eine Partei und für jede Leistungsspezifikation eine von der entsprechenden Partei angebotene Leistung umfaßt. Diese Informationen werden aus dem Angebotsraum des Katalogs ermittelt.
- **Verhandlungsunterstützung.** Eine Verhandlung wird als das gemeinsame Editieren eines Vertrags als strukturiertes Dokumentes aufgefaßt. Jede Modifikation dieses Vertrages wird im Verhandlungskontext von der jeweils empfangenden Partei als ein Vertragsangebot aufgefaßt, welches wiederum als Gegenangebot oder Ablehnung zurückgesendet werden kann. Die Vertragsverhandlung kann unabhängig vom gemeinsamen Editieren durch ein Konferenzsystem - wie z.B. ein Telefon- oder Videokonferenzsystem - flankiert werden. Die Aufgabe der Verhandlungsunterstützung ist dabei erstens eine konsistente und integrierte Dokumentenbearbeitung, zweitens bietet sie die Möglichkeit, zusätzliche Dienste zur Steuerung der Verhandlung hinzuschalten [CePW98]. Dieses ist zum einen ein Workflow-System zur Verhandlungssteuerung, welches auf der Basis flexibler, gefärbter Petrinetze [Jens92] den Kommunikationsfluß zwischen den Parteien steuert, zum anderen bietet es für jeden Teilnehmer die Möglichkeit, ein individuelles Strategiemodul hinzuschalten, welches – im Rahmen der Definitionen von Verhandlungsrichtlinien – zur Durchführung der Verhandlung von einer Partei beauftragt werden kann [TGML98].
- **Unterstützung des Vertragsabschlusses.** Ein Dokument, welches kollaborativ editiert wurde, kann von den beteiligten Parteien gemeinsam elektronisch signiert werden [Schn95]. Bedingung ist hier die Existenz einer standardisierten externalisierten Repräsentation des Vertrages. Zu diesem Zweck im COSMOS-Projekt eine XML-Repräsentation für Verträge entwickelt worden [GoPr98, COSMOS98]. Wenn menschliche Teilnehmer an der Vertragsverhandlung beteiligt sind, ist es erforderlich die Funktionen einer natürlichen Unterschrift (Warnfunktion, Abschlußfunktion, Authentisierung, etc. [HaBi93]) auf das elektronische Medium zu übertragen. Daher folgt diese COSMOS-Komponente dem Motto „What you see is what you sign“: Eine in standardisierter Weise reproduzierbare grafische Repräsentation des Vertrages dient als Grundlage der Unterzeichnung.
- **Abwicklungsunterstützung.** Schließlich wird ein Workflow-System eingesetzt, um die Ausführung von Aktivitäten durch vertraglich spezifizierte Parteien in entsprechender Reihenfolge auszuführen. Dabei sind zwei Formen der Unterstützung möglich: bei *informellen Aktivitäten* (welche durch den menschlichen Benutzer durchgeführt werden) notifiziert das Workflow-System die betreffende Partei, daß eine Aktivität zu verrichten ist. Bei formellen Aktivitäten (die vom Workflow-System etwa durch Methodenaufruf ausgeführt werden können) ist der Austausch geeigneter Parameter- und Resultatobjekte erforderlich [MeLL97].

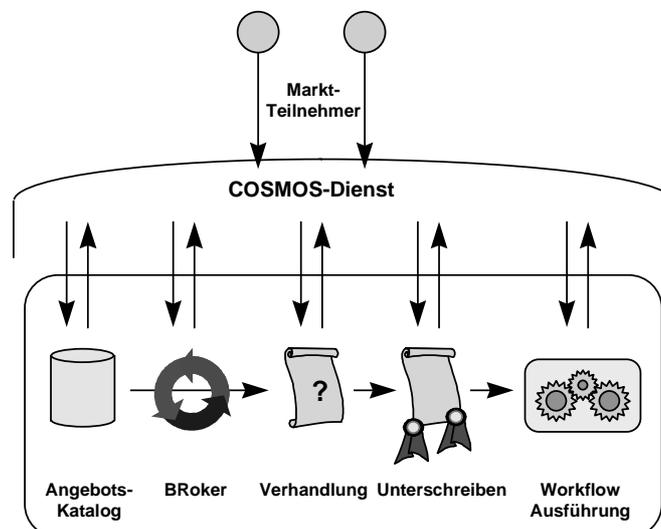


Abb. 50: Funktionen des Electronic-Contracting-Systems

Jeder der erwähnten Dienste kann isoliert angeboten und eingesetzt werden. Die Dienste müssen nicht notwendigerweise vom gleichen Anbieter in Anspruch genommen werden. Der Vorteil einer integrierten Nutzung liegt jedoch in der bruchlosen Übergabe von Objekten zwischen den betreffenden Transaktionsphasen (vgl. Abb. XXX): heute werden Online-Kataloge, Groupware- und Workflow-Systeme als Komponenten für die unterschiedlichen Transaktionsphasen eingesetzt, jedoch mangelt es für die Aufgabe des Electronic Contracting Service an der Integration dieser Systeme. Die COSMOS-Architektur spezifiziert aus diesem Grunde Schnittstellen und Funktionen, so daß eine logische Integration hin zum „one-stop-service“ erreichbar wird.

7.5.6 Weitere Entwicklungen im Bereich elektronischer Verträge

XXX

Surf'N'Sign: Benutzersignaturen auf Web-Dokumenten

XXX

by A. Herzberg and D. Naor

<http://www.almaden.ibm.com/journal/sj/371/herzberg.html>

Von Amir Herzberg (IBM Almaden Labs) stammt die Idee des Surf'N'Sign

This paper discusses the various approaches that could be taken to provide such a mechanism and suggests a solution that provides client commitment on Web documents by means of digital signatures. The architecture and implementation of the solution, called Surf'N'Sign, is outlined in detail. Our design of the solution gives special consideration to the semantics of such a signature and to its proper and secure use on the Web. Its prototype was implemented at the IBM Haifa Research Laboratory as a plug-in to the Netscape Navigator browser and is integrated naturally into the browsing process. It provides a signing mechanism at the client, as well as the capability to archive and preview the signed documents. Surf'N'Sign lends itself to easy integration with existing applications on the Web.

Bei www.semper.org gibt es allerlei dazu. Wir diskutieren ein "split trustworthy graphical user interface". Grundtendenz ist, secure user input/output anzustreben. Geht wahrscheinlich nur ohne Wintel-Komponenten, als mit Display auf separater hardware. Allerdings gibt es wohl Bestrebungen, z.B. bei Siemens und Utimaco, Wintel-Maschinen vom Betriebssystem her sicherer zu machen.

im letzten IBM Systems Journal aufmerksam machen.

Es scheint hier erstmals die Problematik der Unterschrift bezogen auf das zu unterschreibende Dokument nach dem Motto "what you see is what you sign" aufgegriffen zu sein.

Ich finde diese Sicht der Dinge sehr interessant und äußerst relevant fuer die Anwendung von digitalen Unterschriften im elektronischen Waren- und Geldverkehr.

Dienste und Produkte für das Online-Contracting

XXX

Einige Rechtsanwälte und Online-Dienste in den USA bieten bereits einen Service zur interaktiven Erstellung eines Vertrages an. Diese Dienste sind zumeist Web-basiert und erlauben zu bestimmten, festgelegten Rechtsge-

schäften, einen Vertrag in Form eines Frage- und Antwort-Spiels zu komponieren.

Downloadbare SW

Interaktive Dienste

7.6 Zusammenfassung

XXX Gesamtzusammenfassung zu Zu B2B-Commerce!!!

8 Anwendungen im B2B-Commerce

XXX VON HIER AN SUBSTANTIELLE ÜBERARBEITUNG NÖTIG!!!

Bisher wurden im Buch aktuelle technologische und ökonomische Entwicklungen geschildert. Dies ist erst einmal interessant für das Verständnis, *was* Electronic Commerce denn eigentlich ist und *warum* die damit verbundenen Mechanismen zur Zeit so erfolgreich eingesetzt werden. Den Praktiker interessiert hingegen, wie sich diese Mechanismen für sein spezielles Geschäftsfeld einsetzen lassen. Welches Geschäftsmodell „paßt“ zu seiner Branche? Wie kann die bisherige Art und Weise der Leistungserstellung nicht nur verbessert sondern möglicherweise durch einen ganz anderen Ansatz drastisch optimiert werden? Gibt es Verfahrensweisen der Geschäftsmodellierung, die ein erfolgreiches Vorgehen versprechen? Und schließlich: Wie kann ein „Electronic-Commerce-Auftritt“ für das individuelle Unternehmen realisiert werden?

Business Models und Software-Frameworks

Im Bereich des Electronic Commerce lassen sich einige grundlegende Geschäftsmodelle identifizieren, die sich immer wieder hinter unterschiedlichen Branchen und Software-Lösungen verbergen. Ein Geschäftsmodell kann dabei als Rahmenwerk aufgefaßt werden, das – ganz ähnlich den Software-Frameworks – allgemeine Prozeduren und Informationen vorschreibt, ohne dabei das Unternehmen in der Ausgestaltung zu sehr einzuengen. Genauso wie Software-Frameworks der Wiederverwendbarkeit und Interoperabilität von Code dienen, hilft ein Geschäftsmodell, nicht nur Prozesse eines einzelnen Unternehmen zu verbessern, sondern die gemeinsame Interaktion aller beteiligten Geschäftspartner. Als Beispiele seien hier der Ankauf von Regalfläche im Supermarkt durch den Lebensmittelhersteller genannt. Ein Geschäftsmodell dient daher als Schablone, die Rollen, Regeln und Prozeduren für alle Akteure vorschreibt. Dieses Vokabular haben wir bereits im Kapitel über Business-Object kennengelernt, da es dort gerade gilt, Geschäftsmodelle durch Software zu repräsentieren.

Der Ansatz des *Business-Media-Framework* (BMF), der von der Hochschule St. Gallen propagiert wird [XXX], zielt auf eine integrierte Herangehensweise ab, bei der alle Ebenen – Geschäftsbeziehungen, Interne Prozesse, Anwendungssoftware und die Systemebene – letztlich getrieben werden durch das Geschäftsmodell, d.h. die oberste Ebene. Nach dem BMF

XXX BMF Einfügen

EC-Geschäftsmodelle

Bevor nachfolgende einige Anwendungen und Beispiele zur Praxis des Electronic Commerce aufgezeigt werden, ist es sinnvoll, die Rahmenwerke, die den jeweiligen Geschäftsmodellen zugrundeliegen, zu untersuchen. [AdYe98] zählen dazu folgende Grundmuster für „Business Models“ auf:

1. *Informativer Mehrwert.* Durch Standardisierung und Preisverfall sinkt der Preis der Information und damit auch die Kosten, Informationen anzubieten. Geschäftsmodelle mit informativem Mehrwert liefern zusätzlich zu einem gebenen Produkt weitere Daten, die mit ihm in Verbindung stehen. Dies können die Rezensionen von Amazon.Com sein oder die redaktionelle Integration von Online-Malls. In jedem Fall wird eine Geschäftsbeziehung dadurch intensiviert, daß mehr Information zu einem sichereren Kauf führt (wegen der Buchrezension) oder dadurch, daß durch einen Kauf zusätzlich Information erworben wird (z.B. durch den Eintritt in eine Online-Community nach einem Bücherkauf). Informativer Mehrwert kostet den Anbieter im Extremfall nichts. Wenn eine Mindestgröße der Community erreicht ist, emergiert aus den Benutzerprofilen Information, die automatisch für den Feedback zurück in das System genutzt werden kann. Implizite „Trampelpfade“, die sich durch die Navigation von Web-Seiten bilden, können beispielsweise durch eine entsprechende Server-Software explizit gemacht werden.
2. *Wechsel von Geschäftsbeziehungen.* „Wechsel“ ist hier in unterschiedlicher Weise zu interpretieren. Zunächst ist der Wechsel zwischen Geschäftspartnern gemeint. Dies wird z.B. durch Auktions- oder Ausschreibungssysteme unterstützt. Zweites ist mit „Wechsel“ die Geschwindigkeit verbunden, in der Geschäftsbeziehungen wechseln. Früher ist ein Kunde kaum zwischen Automobilmarken gewechselt, entweder war man BMW-, Mercedes- oder Opelfahrer. Heute wechselt fast jeder Fahrer den Hersteller, wenn ein neues Auto gekauft werden soll. Gleiches gilt für Tankstellen, Banken, PC-Hersteller. Durch die Standardisierung der Kommunikation sowie juristischer und geschäftlicher Beziehungen ist ein Wechsel kalkulierbarer und profitabler ge-

worden. Schließlich kann sich der „Wechsel“ qualitativ auf die Geschäftsbeziehung auswirken: Wenn der Händler zum Makler wird oder der Privatkunde dem Online-Dienst seine Profil verkauft, dann bedeutet dies eine Reorganisation von Rollen sowie Zahlungs- und Güterströmen.

3. *Customization*. Dieses Model lebt vom Angebot maßgeschneiderter Produktvarianten. „Customizing“ berührt die Ebene der Kauftransaktion genauso wie die der Fertigung. Während üblicherweise die Produktspezifikation auf den Kunden ausgelagert, ist für den Produktions- und Logistikbereich Software erforderlich, die mit hohem numerischen Aufwand die Fertigung und Auslieferung so steuert, daß optimale Losgrößen erzielt werden.
4. *Internet-Demographie*. Während in den ersten Jahren der Internet-Popularität der junge, männliche Surfer mit Universitätsabschluß als Kunde dominierte, ist in den folgenden Jahren der Anteil der dreißig- sechzigjährigen sowie der der Frauen drastisch gestiegen. Sogar fünf- bis zehnjährige sind inzwischen als Zielgruppe im Internet identifizierbar. Mit diesem Zuwachs neuer Teilnehmer bieten sich den betroffenen Anbietern immer wieder neue Möglichkeiten, als erster diese Zielgruppe zu bedienen. Dies gilt auch für Online-Communities, die sich aus Schülern, Frauen oder Älteren zusammensetzen kann. Für diesen Bereich hat das vom Bundespräsidenten Dr. Herzog initiierte Projekt „Ein Leben lang lernen“ beachtliche Anschubleistung geliefert. So zielt das Teilprojekt „Fit für das Informationszeitalter“ auf die Communities der Arbeitslosen Jugendlichen und der Senioren ab (XXX FIT-URL).
5. *Neue Informationskanäle*. Die Infrastruktur des EC liefert eine weitere Ursache für den Wandel der Geschäftsmodelle: Die Nutzung des Internet erlaubt es Geschäftspartnern in qualitativ neuartiger Weise zu kooperieren. Kommunikation findet nicht mehr 1:1 oder 1:N statt, sondern ohne nennenswerten Mehraufwand N.M. Banner-Tauschringe, Eintrags- und Pressemitteilungsdienste dienen hierbei als Beschleuniger der Kommunikation. Hierbei ist es umgekehrt ein Anreiz, in der möglichen Nachrichtenflut die Information herauszuselektieren, die für den betroffenen Teilnehmer von Bedeutung ist. Auch in diesem Umfeld tummeln sich Unternehmen, die Filteranwendungen oder Content-Managementsysteme anbieten, mit deren Hilfe Metainformation genutzt wird, um dem Empfänger eine „intelligente“ Vorauswahl anzubieten.
6. *Rechtliche Rahmenbedingungen*. Der Handelsverkehr erfolgt nicht ohne Regeln, so daß Technologie erforderlich wird, mit deren Hilfe der Handel mit dem regulatorischen Rahmen abgestimmt werden kann. Shop-Software muß beispielsweise die Steuergesetzgebung beachten, wenn international verkauft wird. Weitere Software ist erforderlich, um Online-Vertragsabschlüsse verbindlich zu machen, damit eine online-Flugbuchung nicht hinterher vom Anbieter oder Kunden abgestritten werden kann. Wie bereit weiter vorne erwähnt, sind Datenschutz-, Verbraucherschutz- und Signaturgesetze zu berücksichtigen, die jedoch den Anbietern entsprechender Softwaresysteme neue Chancen eröffnen. Da noch nicht abzusehen ist, wann und wie diese Regulierungsmaßnahmen abgeschlossen werden, ist noch alles offen bzgl. entsprechend angepaßter Geschäftsmodelle. Man beachte hierbei die grundsätzlichen Unterschiede der Free-Economy oder der Vollkasko-Wirtschaft.
7. *Technologische Innovationen*. Dies ist der treibende Faktor, der z.T. unerwartete Verzerrungen im Markt verursachen kann. Die Verfügbarkeit eines MP3-Players sowie die zunehmende Verbreitung legaler Audio-Clips im Internet greifen das komplette Musikgeschäft an. Für das Jahre 2002 kann prognostiziert werden, daß MP3-Player für weniger als 100 DM angeboten werden. Diese Geräte besitzen eine Kapazität von bis zu 3 Stunden. Neue Audio-Clips können über ADSL geladen werden. Dabei beträgt die Ladezeit zwanzig bis dreißig Sekunden. Vor diesem Hintergrund erscheint die heutige Musikbranche antiquiert. Wozu benötigen wir noch den Vertrieb von CDs? Oder Produzenten und Musik-Verlage? Während die EC-induzierten Verzerrungen im Musikbereich sicherlich zu den dramatischsten gehören werden, werden sich technologische Innovationen in anderen Branchen ebenfalls so auswirken, daß das gesamte Beziehungsgeflecht der Geschäftspartner ins Wanken geraten kann.

Wie auch immer, ein EC-Geschäftsmodell muß immer festlegen, wer der Kunde ist und auf welche Weise das Unternehmen Umsatz und Gewinn generiert. Was wird verkauft und was wird kostenlos zur Verfügung gestellt? Folgt das Unternehmen der Vollkasko-Wirtschaft oder der Free-Economy? Handelt es sich um ein vollständig neues Marktsegment (etwa: P3P-Software) oder um eine Optimierung oder Umgestaltung existierender?

Beim Electronic Commerce ist dies nur selten von Beginn an klar. Fast nie kann ein Break-Even-Point vorausbestimmt werden. Wenn BOL 150 Millionen Euro investiert, um gegen Amazon.Com anzutreten, wieviele Bücher müssen verkauft werden, um daraus ein rentables Vorhaben zu machen? Mit welchen Tricks wird sich Amazon diesen Angriff parieren? Und wie ist der kommerzielle Wert einer „Community“ zu berechnen. Kann BOL Amazon die Leser-Community abwerben? Oder behalten am Ende diejenigen Recht, die von der „The-Winner-takes-it-all-Economy“ sprechen, also eine Monopolisierung in hochspezialisierten Märkten.

Diese Fragen können hier nicht generell beantwortet werden. Es lassen sich bestenfalls für ein gegebenes Unter-

nehmen wirtschaftliche und technologische Perspektiven aufzeigen. Aus diesem Grunde sollen im folgenden einige Geschäftsmodelle angeführt werden. Dies ist ein Schnappschuß einer Weltwirtschaft auf dem Wege zur Internet-Ökonomie.

8.1 Supply-Chain-Management

In diesem Bereich helfen EC-Mechanismen, Prozesse entlang der Zulieferkette zwischen Unternehmen zu verbessern. Der EC-Einsatz hilft hierbei den Einkaufsabteilungen, den Beschaffungsbedarf eines Unternehmens zum richtigen Zeitpunkt zu erkennen und beim Zulieferer rechtzeitig Kapazitäten zu reservieren. Dazu zählt ein präzise Überwachung des Einkaufsverhalten eines Unternehmens. Oft zitiert wird das Unternehmen Wal-Mart, einer der internationalen Spitzenreiter im Beschaffungsbereich. Wal-Mart ist eine amerikanische Supermarkt-Kette, die in den letzten Jahren drastisch expandiert ist und auch begonnen hat, in Europa Fuß zu fassen. Bei Wal-Mart werden Abverkäufe an den POS-Terminal direkt an den Lieferanten gemeldet, so daß dieser in Echtzeit den Lagerbestand des Geschäfts verfolgen kann.

Generell liegt im Beschaffungsbereich ein erheblich Potential bei der Nutzung des Internet: General Electric – international eines der profitabelsten und innovativsten Unternehmen – deckt seinen Beschaffungsbedarf über das Internet bereits im Werte von über 1 Milliarde Dollar jährlich.

Als eine der Schlüsseltechnologien tritt hierbei der elektronische Datenaustausch (EDI) in Erscheinung. Dies muß sich jedoch nicht notwendigerweise in Form von EDIFACT ausdrücken, sondern kann auch in Internet-gerechter Form, wie z.B. auf der Basis von XML und E-Mail erfolgen. Vorreiter ist auch hier wieder die Automobilbranche, in der sich innerhalb kurzer Zeit in den USA der Automotive Network eXchange (ANX) etabliert hat. Die großen drei Automobilhersteller DaimlerChrysler, Ford und General Motors haben ein Extranet eingeführt, das zwischen ihnen und ihren zehn größten Zulieferern besteht. Damit sollen kostspielige und schwer wartbare EDI-Anwendungen abgelöst werden, die bisher für Inkompatibilitäten zwischen unterschiedlichen Herstellern sorgten. Das ANX basiert technologisch auf Internet-Standards, kann jedoch organisatorisch als VAN bezeichnet werden, da der Betreiber von den Nutzer eine Nutzungsabhängige Gebühr für die sichere Zustellung von Nachrichten fordert. Durch die gegenseitige Nutzung von Beschaffungs- und Lieferinformation soll die Integration zwischen den Geschäftspartnern noch erheblich optimiert werden können. Die ANX-Betreiber versprechen sich von dieser Maßnahme eine jährliche Kostensenkung von über einer Milliarde Dollar für die gesamte US-Automobilindustrie.

SAP und DEC setzen Internet-EDI ein, um Verkaufsautomaten nachzufüllen, wenn die „Lagermenge“ einen Bestellpunkt unterschreitet [Crai97]. Dabei meldet ein eingebetteter Computer im Automaten jeden Verkauf an das Auslieferungslager. Damit steht dem Anbieter Echtzeit-Information nicht nur über den Lagerbestand, sondern auch über die zeitliche Verteilung des Verkaufs zur Verfügung. Durch die Nutzung von Standard-Technologie werden gleichzeitig die Investitions- und Betriebskosten der Automaten und des Lagers drastisch reduziert.

8.2 Handel

Im Bereich des Handels gelten insbesondere die bereits diskutierten Prinzipien des Pooling und der Atomisierung.

Automobilhandel

Der Automobilhandel geht dazu über, Autos als frei gestaltbares Produkt über das Web zur Verfügung zu stellen. Dies war natürlich bisher auch im Rahmen der Definition und Fertigung von Produktvarianten möglich, jedoch nicht über das Internet. So kann man sich einem Smart über den Web-Browser mit Java-Applet bzgl. der Farbgestaltung selbst konfigurieren. Der Kunde erhält ein sofortiges Feedback über den individuellen Gesamtpreis und kann in Ruhe, ohne dem psychologischen Druck eines Händlers ausgesetzt zu sein, Lieblingsvarianten ausprobieren. Dieser Detailreichtum kann dem Prinzip der Atomisierung zugeordnet werden, da der Kunde vollständig in die Zusammenstellung eines Produkts eingreifen kann.

Das Prinzip des Pooling greift bei neuen Brokerage-Modell, bei denen sich die Rolle des Händlers vom klassi-

schen Vertriebspartner zum „neuen Intermediär“ wandelt. Klassisch hat der Händler bei Hersteller bestellt, wenn ein Kunde ein neues Fahrzeug beauftragt hat. Evtl. konnten einige Fahrzeuge vorgehalten werden, jedoch nur im Rahmen dessen, was der Händler bereit ist, an finanziellen Mittel zu binden. Der „neue Händler“ könnte etwa folgendermaßen verfahren: Er bietet ein Kontingent an Fahrzeugen mit einem Ausstattungsvorschlag an. Dabei kauft er es jedoch nur, wenn sich der garantierten Abnahmen gewiss sein kann. Dies könnten beispielsweise 200 Mercedes SLK sein, die als Kontingent für 25% Rabatt eingekauft werden. „Electronic Commerce“ kommt ins Spiel, wenn diese Fahrzeuge über das Internet angeboten werden und ein Mechanismus genutzt wird, der Anfragen seitens der Kunden mit dem Angebot des Händlers so in Einklang bringt, daß am Ende eine Lieferung von 200 Fahrzeugen an 200 registrierte Käufer stattfindet. Als Vermittlungsinstrument ist hier ein neutraler Katalog erforderlich, der jedoch weit über die technischen Möglichkeiten einer Online-Mall á la Intershop hinausgeht. Ein solches Marktplatzsystem würde nicht nur den 1:1-Verkauf unterstützen, sondern grundsätzlich das Entstehen der skizzierten Einkaufs- und Verkaufsgemeinschaften. Eine wichtige Voraussetzung ist hierfür jedoch eine technische Unterstützung, welche einen juristisch sicheren Geschäftsabschluß unterstützt.

Am 29. März 1999 versteigerte das Unternehmen Sixt erstmals gebrauchte Fahrzeuge über das Internet. Dabei wurde die holländische Auktion angewendet, bei der eine anfängliche Preisforderung alle 10 Sekunden um 250 DM zurückgenommen wird. Wer als erster kauft erhält den Zuschlag. Einen anderen Ansatz wählt das Unternehmen Priceline (www.priceline.com), über das der Käufer einen Preis nennt, zu dem ein passendes Angebot ermittelt wird. Dieser Service stand ursprünglich für Autos, Flüge, Hotelzimmer und Hypothekenkredite zur Verfügung. Mit der Zeit werden weitere Produkte in das Angebot aufgenommen.

8.3 Banken und der Wertpapier-Handel

Bereits seit einigen Jahren unterstützen Banken die Kontoführung über T-Online und neuerdings auch über das Internet. Hierbei lag der gemeinsame Nenner des Internet-Zugangs auf der Ebene des WWW bzw. einer eigenen Masken- und Interaktionsgestaltung, d.h., jede Bank konnte ihre proprietäre Schnittstelle realisieren. Neuere Standards wie das HBCI (Homebanking Computer Interface) erlauben jedoch Interoperabilität zwischen beliebigen Clients und allen Banken, bei denen ein Kunde ein Konto eingerichtet hat. Eine zukünftige Entwicklung der Homebanking-Software könnte folglich zur Multibankenfähigkeit führen: Der Kunde nutzt die Software, um Anfragen an die Banken zu leiten und anschließend von allen Wettbewerbern Angebote einzuholen. Dabei könnte es sich um ein Anlagegeschäft, einen Hypothekenkredit oder die Eröffnung eines Kontos handeln. Auch hier würde sich dann der Trend zur Atomisierung und Personalisierung fortsetzen.

Ähnliches gilt für den Investmentbereich: Discount-Broker, die wie z.B. Consors (<http://www.consors.de>), Charles Schwab (www.schwab.com) oder E*Trade (www.e-trade.com) nur noch per Internet, T-Online und Telefon kontaktiert werden, bieten ihre Dienste zu Provisionen an, die bei einem Bruchteil der bisherigen Bankprovision liegen. Wertpapiere lassen sich damit von Privatpersonen innerhalb einzelner Tage kaufen und wieder verkaufen. Als zentrale Schaltstelle tritt dabei immer noch die Wertpapierbörse auf. Auch für diesen Bereich zeichnet sich bereits die nächste Revolution ab: Warum müssen Wertpapiere an der Börse gehandelt werden, es könnte doch das herausgebende Unternehmen selbst die Halter seiner Aktien verwalten – selbst wenn diese Anonym bleiben wollen.

Bisher war der zentralisierte Handel vorteilhaft, da die erforderliche Infrastruktur und der Marktzugang nur für wenige, permanent etablierte Teilnehmer wirtschaftlich war. Außerdem wäre die nötige Markttransparenz nicht gegeben, würden die Aktien eines Unternehmens direkt zwischen individuellen Käufern und Verkäufern gehandelt werden. Mit der zunehmenden Kostenreduktion bei Kommunikation und Transaktionen kann ein Unternehmen sich heute jedoch selbst um die Verwaltung seines Aktienbestandes und seiner Aktionäre kümmern – oder zumindest einen Dienstleister beauftragen, der diese Aufgabe erledigt. Genau in diesem Bereich treten zur Zeit Unternehmen wie beispielsweise NetIPO (www.net-ipo.de) auf, die – an der Wertpapierbörse vorbei – den Aktienhandel eines einzelnen Unternehmen betreiben.

Online-Dienste wie Virtual Wallstreet (<http://www.virtualwallstreet.com>) moderieren dabei Virtual Communities im Investmentbereich. Hier stehen Einzelpersonen als Investoren einzelnen Start-Up-Unternehmen gegenüber, die ihrerseits Beteiligungen anbieten. Ein solcher Marktplatz spielt sich vollständig jenseits der Banken und Börsen ab. Bisher hing die IPO – Initial Public Offer – von einer Vielzahl Beteiligter wie Emissionsbanken, Wirtschaftsprüfungsgesellschaften und Rating-Agenturen ab. Die damit verbundenen Kosten waren nur tragbar, wenn das Unternehmen bereits eine Größe erlangt hat, bei der solche Kosten tragbar waren. Im Zeitalter des Electronic Commerce lassen sich jedoch die Kosten der Aktienemission drastisch reduzieren. Im Prinzip könnte jedes Kleinunternehmen, das seinen Investoren glaubhafte Expansionspläne darlegen kann, Aktien emittieren. Regulatorisch hat der Gesetzgeber hier jedoch einige Riegel vorgeschoben: Zum einen muß das Unternehmen in der

Rechtsform der Aktiengesellschaft firmieren, zum anderen ist eine behördliche Zulassung erforderlich, bevor der Börsengang erfolgt.

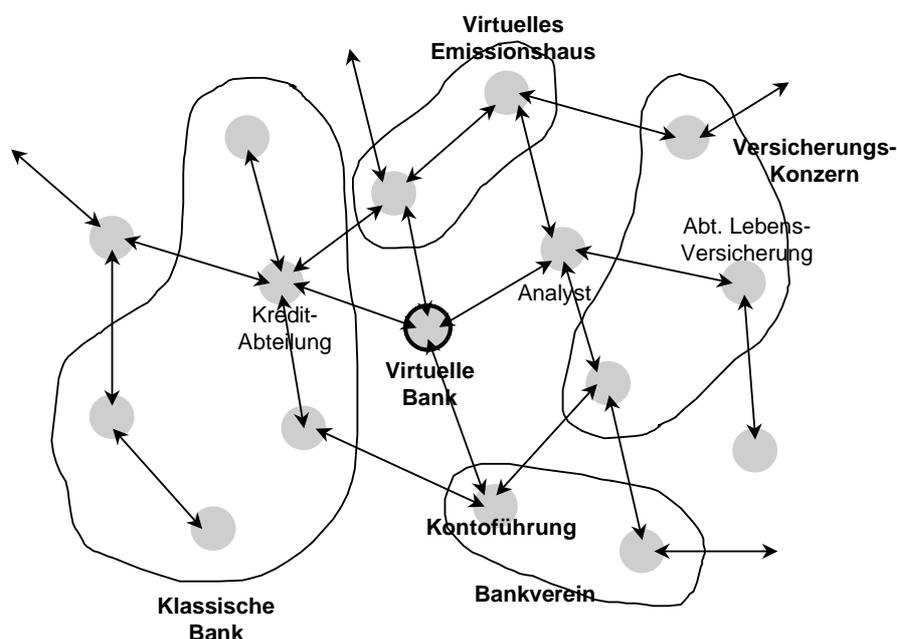
Der nächste Schritt könnte im Zuge der fortschreitenden Atomisierung die Moderation von Privatinvestments sein: Wenn ein Bauherr ein Mehrfamilienhaus bauen möchte und dazu eine halbe Millionen Euro an Fremdkapital benötigt, so könnte er 100.000 Aktien im Werte von 5 Euro herausgeben. Beim Direct IPO würden sich Investoren registrieren lassen – zum Beispiel, indem sie 6 oder 7 Euro je Aktie bieten, Angebot und Nachfrage sind hierbei gesteuert durch Faktoren wie Vertrauen, Fungibilität und erwartete Rendite. Entsprechend der Renditeerwartung durch Mieteinnahmen kann der Aktienwert anschließend steigen oder fallen. Wenn sich in der Zukunft sichere Privathandelssysteme etabliert haben, die für derartige Mikroinvestments die gleiche Provision berechnen wie heute ein Online-Broker, dann lassen sich in dieser Branche alle wesentlichen Merkmale des Electronic Commerce nachvollziehen: Vertrauensökonomie, Sicherheits- und Zahlungsinfrastruktur, Aufmerksamkeitsökonomie, Atomisierung, Disintermediation, Re-Intermediation, Adhocracy usw. Diese Faktoren wirken sich im Wertpapierbereich als typische Soft-Good-Branche besonders drastisch aus.

Wo bleibt dabei das „Alleinstellungsmerkmal“ der klassischen Bank, wenn man sich dieses Szenario im Kontext der Free-Economy vorstellt? Ist sie Vertrauensträger? Kaum, da jedes andere Markenunternehmen den gleichen Service anbieten könnte. Sogar ein nur im Stadtteil bekanntes Unternehmen könnte als Betreiber auftreten. Ist die Bank zur Abwicklung der Transaktionen erforderlich? Nein, denn in der Free-Economy ist keine Lizenz zur Herausgabe oder Verwaltung von Geld erforderlich. Höchstwahrscheinlich könnte die Bank in die Rolle der Rating-Agentur schlüpfen, da ihre Mitarbeiter erfahren sind in der Analyse von Finanzinformationen und Investitionsplänen. Aber ist dafür die gesamte Bank erforderlich oder nur einzelne Mitarbeiter?

Ein drastisches Beispiel wurde im Manager-Magazin vom März 1999 präsentiert: In einem kleinen Büro in Dublin richten vier ehemalige KPMG-Berater und Bankexperten mit der „ENBA“ die erste virtuelle europäische Bank ein. Von der Kontoeröffnung über den Aktienhandel und der Kreditvergabe zum zur Kontoauflösung erfolgt hier jede Transaktion ausschließlich über das Internet. Im Gegensatz zur einer traditionellen Bank werden sämtliche Finanzdienstleistungen auf Drittanbieter ausgelagert. Hierbei macht sich die ENBA Überkapazitäten der Konkurrenz zunutze, um Aktienorders oder die Kontoführung abzuwickeln. Die Dienstleistungen, die ENBA damit anbietet, erfordern keinen intensiven Personal- oder Kapitaleinsatz – lediglich Anbindung leistungsfähiger Rechner an das Internet. Gleichzeitig skaliert dieses Konzept mit einer steigenden Kundenzahl, da aufgrund der vollständigen Automatisierung kaum zusätzliche Mitarbeiter erforderlich sind. Somit agiert die ENBA als Transaktionsportal für Finanzdienstleistungen und lebt von der Integration ihrer Kunden mit den Diensten ihrer Kooperationspartner.

Neben der eingenen virtuellen Bank, werden die gleichen Dienstleistungen nach dem Mall-Konzept auf für Dritte angeboten. Wenn vielleicht noch nicht 1999, so ist doch für die nächsten Jahre zu erwarten, daß ein Unternehmen, das eine Bank gründen möchte, dies quasi „per Knopfdruck“ über die Mall von ENBA leisten kann.

Analog zur Abbildung XXX (virtuelle Organisationen) stellt die virtuelle Bank lediglich eine Funktionale Einheit in einem Netz aus Bankdienstleistungen dar:



8.4 Amazon.Com

XXX Siehe Economist, Quelle [87] bei Yesha et al. , „The Economist Electronic Commerce Survey: In search of the perfect market“In: The Economist, May 10, 97

8.5 Weiteres...

8.5.1 Die Zukunft des Business-to-Business-Commerce

Faßt man die bisherigen Abschnitte zum B2B-Commerce zusammen läßt sich quasi als „Fingerprint“ folgendes sagen:

„Die Zukunft des B2B-Commerce liegt in der komponentenbasierten Ad-hoc-Konfiguration von Extranet-Anwendungen, die mit Hilfe elektronischer Verträge spezifiziert und unterschrieben, mit Hilfe standardisierter Workflowsysteme aktiviert und zur Ausführung gebracht werden und auf der Basis flexibler Austauschformate mit standardisierter Syntax und Semantik kommunizieren“.

Bis zur Realisierung solcher integrierten Geschäftssysteme kann es jedoch noch lange dauern – auch wenn die zuvor dargestellte Technologie bereits heute zur Verfügung steht. Die größte Schwierigkeit dürfte nach wie vor in der Durchsetzung einer allgemeinen Standardisierung liegen. Dies betrifft weniger den softwaretechnischen Bereich als den der Kommunikation. Während sich proprietäre Geschäftsanwendungen wie SAP oder San Francisco mit gewissem Aufwand kapseln und damit in ihren gegenseitigen Schnittstellen vereinheitlichen lassen, ist die Standardisierung von Inhalten weitaus komplexer.

XXX

9 Wohin führt Electronic Commerce?

Elektronische Rechnungen gleich elektronisch zahlen **Fehler! Verweisquelle konnte nicht gefunden werden.**]

Zeitungen im Internet: Wie finanzieren? **Fehler! Verweisquelle konnte nicht gefunden werden.**]

Sexanbieter als Pioniere des Electronic Commerce? **Fehler! Verweisquelle konnte nicht gefunden werden.**]

9.1.1 Die Zukunft der Bank im Internet

Im Kern ist die Bank vor allem eine Buchungsmaschine für Zahlungstransaktionen. Alle weiteren Funktionen stellen eine Schnittstelle zwischen diesem Kern und dem Kunden dar. Einzahlungen und Entnahmen werden über die Filiale oder das Internet abgewickelt. Interbankennetze werden für die sichere Abwicklung von Zahlungstransaktionen betrieben. Der Aktienhandel umfaßt Analyse- und Beratungsdienste die wieder in persönlicher oder automatisierter Form dem Kunden angeboten werden. Kredite werden Privat- und Firmenkunden angeboten und wiederum über die Zentrale Buchungsfunktion ausgezahlt und getilgt. Schließlich tritt die Bank als Akteur im Wertpapierhandel auf – im eigenen Namen oder im Namen ihrer Kunden. Diese Liste müßte noch beliebig verlängert werden, um alle Geschäftsfelder abzudecken, die eine heutige Großbank umfaßt. Bis zur Mitte der neunziger Jahre war es das Bestreben der meisten Großbanken, zu diversifizieren und durch die Integration weiterer Geschäftsfelder alle denkbaren Finanzdienstleistungen anzubieten. Seit einigen Jahren treten jedoch neben die klassische Großbank viele hochspezialisierte Kleinanbieter, die sich auf nur wenige Kernprodukte beschränken.

Ein Online-Broker wie z.B. Consors in Deutschland oder Charles Schwab (XXX?) in den USA konzentriert im wesentlichen sich auf die Abwicklung von Wertpapiertransaktionen der Kunden. Die Aktualität der Kursberichte sowie die geforderte Provision sind im Vergleich zu traditionellen Banken konkurrenzlos. Kleine Privatbanken mit weniger als 100 Mitarbeitern würden ein Vielfaches ihrer heutigen Mitarbeiterzahl benötigen, um die vollständige Abwicklung von Zahlungstransaktionen mit einem eigenen Rechenzentrum durchzuführen. Die Lösung liegt im Outsourcing, das hier nicht nur den Betrieb des Rechenzentrums betrifft, sondern das komplette Transaktionssystem. Ein Bankkunde mag zwar organisatorisch der Bank gegenüberreten, wenn er sich über das Internet einloggt, de facto wird der gesamte Zahlungsverkehr jedoch von einem anderen Betreiber wie z.B. dem Bankverein (XXX?) abgewickelt. Der Bankverein selbst ist damit ein Dienstleister, der sich auf eine andere Kernkompetenz spezialisiert hat. Eine „Mikrobank“ mit weniger als 20 Mitarbeitern wurde kürzlich von ex-KPMG-Mitarbeitern in Irland gegründet [Manager-Magazin]. Diese Bank betreibt lediglich einen Web-Server in einem angemieteten Büro. Auf kostspieliges Presige wird vollständig verzichtet, so daß die Investitionskosten minimal sind. Bedient werden Kunden in ganz Europa, insbesondere im Bereich des Investment-Banking. Daneben soll jedoch das gesamte Sortiment der Bankdienstleistungen unterstützt werden – nur mit dem Unterschied, daß quasi bereits hinter dem Web-Server die Transaktion an einen Outsourcing-Partner weitergeleitet wird.

... XXX

Auch im Bereich der Banken finden sich die Varianten „klein und schnell“ und „groß und schlagkräftig“ wieder. Das Gegenmodell zur Mikrobank liegt in der Diversifikation in andere Branchen hinein. Einer Meldung der Süddeutschen Zeitung zufolge will Die Deutsche Bank „...die Kabelfernsehnetze der Telekom mit insgesamt rund 18 Millionen angeschlossenen Haushalten übernehmen. Nach Informationen der Süddeutschen Zeitung liegt der Telekom ein schriftliches Kaufangebot vor, in dem die Bank sich bereit erklärt, bis zu 9 Milliarden Mark zu zahlen. Deutschlands führendes Finanzinstitut plant, das Kabel zum Multimediantz mit Internetzugang auszubauen ...“ [SZ, 21.11.98].

Obwohl bei einer Integration des Bankgeschäfts mit dem des Netzbetriebs keine direkten Synergien zu erkennen sind, liegen sie sicherlich bei der Schaffung einer Vertrauensinfrastruktur. Wenn ein Multimedia-Online-Service von der Bank selbst betrieben wird, und Finanzdienstleistungen darin integriert werden, kann die Rolle der Bank als Vertrauensstifter durchaus Sinn machen.

Aus der Verallgemeinerung kann man grundsätzlich zwei Schlüsse ziehen: Erstens bietet sich das Modell „Engagement als Vertrauensträger“ für alle Markennamen an, so daß im Prinzip auch DaimlerChrysler und die Esso das Netz kaufen könnten. Zweitens könnte sich die Bank in diversen anderen Bereichen engagieren, die besonders vertrauenssensitiv sind. Dies ist sicherlich einer der Gründe für die Übernahme des Hamburger TC TrustCenter durch die Commerzbank.

Nach wie vor bringt die Deutsche Bank Ecash in Umlauf – zwar nicht als Wahrung, jedoch als Zahlungsverfahren mit dem technischen Potential fur eine unabhangige Privatwahrung. Auch hier konnte sich eine Bank – je nach zukunftiger Gesetzgebung – in Richtung „Notenbank“ diversifizieren.

9.1.2 Handel

Das Re-engineering von Organisationen

Die meisten Unternehmen versuchen lediglich Teilfunktionen des gesamten Geschafts auf das Internet zu *ubertragen*. Dies gilt z.B: fur den Einkauf, den Vertrieb

Optimism over E-commerce application growth is registered by both the Romtec and Deloitte & Touche surveys, yet it is currently having very little impact on existing organisations in Europe. While there are examples of software distributors turning themselves from physical to Internet-only companies, there are few, if any, in other European industry sectors. In the majority of cases, Internet-only companies are new start-ups, and many of them are intermediaries in new market areas, that is, “middlemen”, providing Internet-based services that enable buyers to find sellers, and vice-versa, in particular markets.

The start-up intermediary position is a lucrative one: such companies typically turn over a high volume of business with very low overheads. Quixell was set up in September 1997 to auction computer products, and now, as Europe’s largest online auction company, with an expected turnover in its first year of trading of 4.2 million ECU and 20 staff, auctions a growing range of items, including consumer electronic products, jewellery and timeshare holidays.

Intermediaries will play an increasingly vital economic role over the next two to five years in matching suppliers and customers, potentially creating a competitive environment in favour of the smaller, more “agile” and niche supplier

over larger businesses. At this point, E-commerce will begin to have an impact on many more organisations.

Today, when businesses, large and small, open up a new channel to market through the Internet, they are typically doing so without significantly changing their existing business, or taking on new staff. Cedlerts Fisk, for example, services orders to consumers, which are taken via the Internet, in the quiet moments when its staff are not fulfilling orders for business customers. Surgicon, a small UK distributor of surgical products, has redeployed staff as a result of putting an online order and fulfilment capability in place.

Internet-based E-commerce pilot operations in food retail are often add-ons to the rest of the business. Such pilots are proving uneconomic to roll out on a large scale, and it is likely that companies will have to adopt a different

9.1.3 Freier Handel mit Kundendaten?

Wie oben erwähnt, lassen sich verschiedene Grundlagen für ein EC-Geschäftsmodell finden. Eine davon liegt in der Auswertung von Profilinformaton und in der Konzentration auf lukrative Kunden. In den USA, wo kaum regulatorische Rahmenbedingungen den freien Handel beeinträchtigen, kann eine Bank einen unerwünschten Kunden ablehnen. Heute kann sie noch nicht vollständig erkennen, ob ein Kunde profitabel ist oder nicht – lediglich anhand von Auskunften zur ist eine grobe Klassifikation möglich. Ob er die Bank jedoch mit vielen kleinspreisige Transaktion quält oder sein Kontostand unprofitabel ist, kann nur von der Bank selbst, nicht jedoch von anderen eingesehen werden. Wenn in Zukunft Profildaten beliebiger Präzision frei gehandelt werden können, besteht für eine Bank, bei der ein Neukunde ein Konto einrichten möchte, damit ein Instrument, das hilft, unprofitable Kunden auszusortieren.

Electronic Commerce kann hier zu einer Diskriminierung der Bürger in Abhängigkeit von ihrem Einkommen führen. Da man heute ein Girokonto zum Mindeststandard einer bürgerlichen Existenz zählen kann, treffen hier die zwei Grundansätze des Gesetzgebers aufeinander: Regulation versus laissez-faire.

"In the brave new banking world, the 'unprofitable' customer will find that bankers don't want you – or your money..." [XXX]

So heißt es in einer Publikation der US-Bankenindustrie. Der Artikel berichtet über den Einsatz von Profiling- und Customer-Relationship-Software, der für viele Kunden das Aus bedeuten kann. Auf einem Symposium amerikanischer Großbanken in Las Vegas wurde im Dezember 1998 beraten, auf welche Weise der Übergang in eine Welt des „gläsernen Kunden“ geschafft werden kann – ohne eine Rebellion der Kunden heraufzubeschwören.

Im „Bank Rate Monitor“ erschien im Januar 1999 ein Artikel mit dem Titel "Big Banker is Watching" wird der zukünftige Einsatz von CRM-Software erläutert. In dem Artikel wird über die CRM-Software der Epsilon Soft-

ware Development Company berichtet, die „die Internaktion mit der Bankgeschäfte ändern wird – oder ob man überhaupt interagiert.“¹⁶

Bankgeschäft werden zukünftig ausschließlich online oder per Telefon abgewickelt, nicht jedoch über Filialen. Bereits heute denken Banken auch in Deutschland darüber nach wie das Personal, das in den Filialen tätig ist, im Laufe der Zeit abgebaut werden kann. Sie werden nur noch als Ladengeschäft benötigt, das Kunden für Darlehens- oder Anlagegeschäfte aufsuchen. Daneben wird das Vertriebspersonal – ähnlich der Versicherungsbranche – Hausbesuche abstaten. Dies ist weitaus günstiger, als im Innenstadtbereich kostspielige Filialen zu betreiben. Zumindest in den USA wird das Vertriebspersonal dann erfolgsabhängig entlohnt.

Natürlich werden persönliche Daten offiziell nur freiwillig eingefordert, stehen sie jedoch nicht zur Verfügung, wird mit einem niedrigeren Service-Niveau reagiert werden. Der Executive Vice President der First Manhattan Consulting Group's, Seamus McMahon, wird zitiert mit den Worten "you charge them higher fees because you don't want them – make them know they're not welcome." Und weiter unten: "Unprofitable customers will pay an additional price in terms of service. Each time a customer calls or e-Mails a bank, the sales rep need only type his name to view his CRM profile. 'You answer the cash cows first,' said McMahon. 'The losers can wait 20 minutes if they call in a question. The losers will just make you drown.'"

Customer Relationship Management bedeutet, daß Bankangestellte benachrichtigt werden, wenn ein profitabler Kunde ein Kind bekommen hat. Als Teil des Service wird unmittelbar ein Werbegeschenk verschickt – Zusammen mit Hypothekenangeboten für Umbaumaßnahmen im Hause. Verpackt wird dies mit Informationen über Kindergärten und Tagesmütter. Umgekehrt generiert die Software Angebote für Kleindarlehen, wenn es gilt, das Begräbnis eines frisch Verstorbenen zu finanzieren.

Die Liste der Kundendaten kann beliebig fortgesetzt werden: Andere Anbieter schlagen vor, auch „psychographische Daten“ über Hobbies, die politische Einstellung, abonnierte Zeitschriften und „Aktivitäten“ wie Club-Mitgliedschaften, kürzliche Käufe und frequentierte Modeboutiquen zu sammeln. Diese Information wird von Auskunftsdiensten wie z.B. dem amerikanischen Debit Bureau zur Verfügung gestellt. Debit Bureau strebt an, die Granularität demographischer und geographischer Daten auf einzelne Haushalte herunterzubrechen. Damit kann das Einkommensniveau einzelner Straßenzüge und Wohngebiete nicht nur statistisch, sondern erstmals auch aufgrund empirischer Daten von Einwohnern bestimmt werden. Diese Information ist Gold wert – nicht nur für Banken. Wenn nun die Bankfiliale über diese Informationen verfügt, kann sie unerwünschte Kunden bereits am Eingang durch Verwendung biographischer Authentisierungstechniken ermitteln und abweisen. Die meisten US-Banken beginnen bereits heute mit der Einführung von Fingerabdruck-Lesegeräten als ersten Schritt, um unerwünschte Personen fernzuhalten.

Microsoft und die Kunden-ID

Anfang 1999 berichtete die Zeitschrift C'T, daß Microsoft unter bestimmten Umständen Registrierungsdaten von Windows98 unaufgefordert an die Zentrale in Redmont übermittelt und dort in einer Datenbank verwaltet. Ferner konnte nachgewiesen werden, daß diese ID, die auf der Kennung der Netzwerkkarte des PC basiert, ebenfalls in Word-, Excel- und Powerpoint-Dateien verwendet wird. Damit sind alle Office-Dokumente, die im Internet ausgetauscht werden mit dem „Brandmal“ eines PCs gekennzeichnet – ohne daß der Besitzer dies weiß. Da in den USA keine Datenschutzbestimmung existiert, mag dies dort rechtens sein, in Deutschland und in allen Staaten, die die EU-Datenschutzrichtlinie umgesetzt haben verstößt dies gegen lokales Gesetz. Dies gilt auch, wenn der Anbieter in einem Land mit niedrigerem Datenschutzniveau sitzt. Besonders heikel ist die Tatsache daß der US-Ansatz zur Selbstregulierung ebenfalls in die Kritik geraten ist: Microsoft hat sich von TRUSTe bescheinigen lassen, daß die vereinbarten Datenschutzmaßnahmen eingehalten werden. Durch das Brechen dieser Vereinbarung wird das gesamte System der freiwilligen Selbstkontrolle in Frage gestellt. Nachdem US-Datenschutzorganisationen auf diesen Fall aufmerksam wurden, mehrten sich auch dort die Stimmen, die nach einer Mindestregelung verlangten (z.B. www.junkbusters.com).

9.1.4 Trusted Third Parties

Vergleich der Electronic Signature Regulation in versch. EU-Ländern **Fehler! Verweisquelle konnte nicht gefunden werden.**

¹⁶ The Software will "change how you interact with your bank – or whether you interact at all."

Neue Dienste im Internet:

- Zertifizierungsautoritäten (CA)
- Notariatsdienste

9.1.5 Prozessintegration, Interorganisationales Workflowmanagement

Öffentliche Ausschreibungen **Fehler! Verweisquelle konnte nicht gefunden werden.** www/kbd/co/uk

Physische Auslieferung von Produkten

→ FedEx

Business-to-Business-Commerce

9.1.6 Supply-Chain-Management

Logistik-Systeme

Requisitioning, öffentliche Beschaffung

Beschaffung & Beschaffungs-Pooling (→ Querverweis auf Brokerage)

Zitat (hmd_vv.pdf)

Supply Chain Management (SCM)

Eine besonders systematische Abstimmung von Kunden- und Lieferantenbeziehungen unter Ein-schluß von Spediteuren und Lagerhaltern stellt das SCM dar [39]. Die Logistik-Ketten von VU verlangen eine integrierte Planung, Steuerung, Administration und Kontrolle der Güter- und Informationsströme zwischen den Partnern (vgl. vertikale Zusammenarbeit im Abschnitt 2.2). Beispielsweise gestaltete Hewlett-Packard [40] seine Logistik-Ketten, die sich über eine Vielzahl von Produktionsstätten in Asien und Amerika erstrecken, mit Hilfe von Simulationsrechnungen übergreifend neu. Es gelang, die systemimmanenten Schwankungen, wie sie auch als Forrester-Effekte bekannt sind zu beherrschen. Der schnelle Auf- und Abbau solcher Logistik-Ketten in VU stellt besondere Anforderungen an das SCM. Im Zusammenhang zu SCM stehen Methoden wie Continuous Replenishment, Quick Response oder Point-of-Sales-Systeme [41].

Supply chain management is the co-ordination of materials and information flows between companies in the supply chain. This paper discusses the possible implications of supply chain management on virtual corporations and virtual webs. Based on a case study it determines the effects on the supply chain management in the process of the evolution from a single virtual corporation to a vir-

tual web.

...

The International Center for Competitive Excellence (1994) provides following definition:

'Supply chain management is the integration of business processes from end users through original suppliers that provides products, services and information that add value for customers'.

The supply chain is a network of organisations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hand of the ultimate consumer.

The concept of supply chain management extends the logic of integration outside the boundaries of a firm to include suppliers and customers (Christopher 1992).

The activities of supply chain management are the integrated planning, scheduling, administration and controlling of the materials and information flows (Mertens 1995).

To implement supply chain management, some level of co-ordination across organisational boundaries is needed. This includes integration of processes and functions within organisations and across the supply chain.

A driving force behind supply chain management is the recognition that suboptimisation occurs if each organisation in the supply chain attempts to optimise its own results rather than to integrate its goals and activities with other organisations to optimise the results of the chain. Houlihan, Jones and Riley (1985) stated that the objective of supply chain management is to 'lower the total amount of resources required to provide the necessary level of customer service to a specific segment' (Cooper 1997).

Zitate aus HMD:

Supply Chain Management (SCM)

Eine besonders systematische Abstimmung von Kunden- und Lieferantenbeziehungen unter Ein-schluß von Spediteuren und Lagerhaltern stellt das SCM dar [39]. Die Logistik-Ketten von VU verlangen eine integrierte Planung, Steuerung, Administration und Kontrolle der Güter- und Informationsströme zwischen den Partnern (vgl. vertikale Zusammenarbeit im Abschnitt 2.2). Beispielsweise gestaltete Hewlett-Packard [40] seine Logistik-Ketten, die sich über eine Vielzahl von Produktionsstätten in Asien und Amerika erstrecken, mit Hilfe von Simulationsrechnungen übergreifend neu. Es gelang, die systemimmanenten Schwankungen, wie sie auch als Forrester-Effekte bekannt sind zu beherrschen. Der schnelle Auf- und Abbau solcher Logistik-Ketten in VU stellt besondere Anforderungen an das SCM. Im Zusammenhang zu SCM stehen Methoden wie Continuous Replenishment, Quick Response oder Point-of-Sales-Systeme [41].

9.1.7 Web-Billing

9.1.8 Beispiele für Virtuelle Unternehmen

Beispiele

Das am häufigsten aufgeführte Beispiel für diese Stufe ist die Rosenbluth International Alliance [35], illustrierend dafür ist aber auch die IBM-Tochtergesellschaft AMBRA. Ein weiteres Beispiel ist *Lewis Galoob Toys* (vgl. [36], S. 3): Dieser US-amerikanische "Hersteller" von Spielwaren, beschäftigt kaum mehr als 100 fest angestellte Mitarbeiter und vermarktet Waren im Wert von über 50 Mio. \$ (1985). Galoob kauft Produktideen von unabhängigen Erfindern und läßt die Entwicklungsarbeit von selbständigen Ingenieurbüros durchführen. Die eigentliche Herstellung erfolgt durch Subkontrakt-Unternehmen in Hongkong, die ihrerseits arbeitsintensive Funktionen in China ausführen (lassen). Die Fertigprodukte werden durch Spediteure in den USA transportiert und dort über selbständige Vertragsrepräsentanten vertrieben. Selbst Funktionen wie Factoring und Finanzbuchhaltung werden von selbständigen Dienstleistungsunternehmen ausgeführt. Galoob beschränkt sich im Kern auf die strategische Führung dieses Netzwerkes selbständiger Unternehmen, tritt also als Leader-Firma auf. Noch vor wenigen Jahren wurde Galoob von einigen Beobachtern als "[...] very alien business creature" [37, S. 243] angesehen. In der Zwischenzeit ist das Modell aber bereits von einigen Konkurrenten erfolgreich adaptiert worden.

EDI-Verträge für den Zusammenschluß zum VU

Übersetzen:

So, before using EDI the partners have to come to an agreement on the definition of the applied standard. Moreover, critical issues of EDI like data-security and share of responsibility have to be negotiated also. The contract then has the character of a skeleton agreement. Such exchange-profiles are developed by neutral institutions and contain standardised conditions which will be modified into codes. At the beginning of a virtual corporation these codes can be passed directly into an EDI-note.

In conclusion EDI shows very mixed impressions referring to transaction-costs. On one hand, EDI possesses the skills and has reached a state that is able to reduce transaction-costs like handling or execution costs. At the other hand, in many cases special negotiations and agreements about the arranging of used EDI standard and technique are necessary, which causes bargaining costs during the formation of Virtual Organisations. Because of these early costs, the dynamic of Virtual Organisations is reduced. Expense free switching to another partner is a very important feature of Virtual Organisations. But the negotiations mentioned cause very high disincentive costs in dependence from the partner.

Davidow, William H.; Malone, Michael S.: *The Virtual Corporation: Structuring and revitalizing the corporation for the 21st century*. HarperBusiness, New York 1992.

Davidow, William H.; Malone, Michael S.: *Das virtuelle Unternehmen: der Kunde als Co-Produzent*. Campus-Verlag, Frankfurt/Main New York 1993.

Oksana Arnold, Wolfgang Faisst, Martina Härtling, Pascal Sieber: *Virtuelle Unternehmen als Unternehmenstyp der Zukunft?* (→hmd_vv.pdf)

Virtuelle Unternehmen und EDI

Bei der Betrachtung virtueller Unternehmen steht nicht die interne Organisation der partizipierenden Unternehmen oder deren Kompetenz im Vordergrund, sondern vielmehr ihre Flexibilität beim Zusammenschluß und der Bildung von Kooperationsbeziehungen. Heute wird die erforderliche Anpassungsfähigkeit zum einen noch durch "Altlasten" wie z.B. EDI oder SAP beeinträchtigt, zum anderen existiert noch kein Standard, der das Zusam-

menschalten von Teilorganisationen ad hoc von der Ebene der Datenkommunikation bis zur Geschäftsebene erlaubt.

In Figure 3, we show that the trading arrangements from community to community will be different. However, it is possible to describe a business conversation in such a way that the high level process description is common across trading communities. Specifically, the process used by a company to reserve a seat on an airplane for employee business travel should match that of reserving material from a supplier or space in a hospital. This similarity of process exists even though the detail of the information exchanged in the transactions are different.

The notion of the virtual enterprise in the future state model relies upon this distinction between the detailed information exchanged by trading partners and the sequence of events in which the information is used to conduct business. The standards required by the virtual enterprise in the future must be designed to support this separation between data and process.

This model of the virtual enterprise allows any individual enterprise to retain its own essence or competitive advantage within its four walls but at the same time engage in routine business operations with entire trading communities.

The virtual enterprise of the future state vision, is defined by this combination of trading partners interoperating with a series of predefined, multilateral trading agreements.

Existierende Formen:

- Einzelkämpfer
- Unternehmen
- Virtuelle Hierarchie
- Polymorphe virtuelle Hierarchie → ...\economics\Polymorphe Hierarchien als Ausweg

Zitate aus HMD:

Unternehmen weiten die Optimierung der Wertschöpfungskette auf Kunden und/oder Lieferanten aus. Die Integration erfolgt analog der Funktionsintegration der Entwicklungsstufe 1. Die Unternehmen überdenken ihre Außenbeziehungen und erreichen diese Stufe z.B. durch ein Business Network Redesign. So hat Procter & Gamble [30] in seinem Distributionssystem Zwischenhändler und Endverkäufer in die Logistik eingebunden. Dabei zeigt sich, daß z.T. auch neue Aufgaben-zuteilungen vorgenommen werden: Procter & Gamble übernimmt zum größten Teil die Bestellungsabwicklung für seine Kunden. Entsprechende Abmachungen (z.T. in Verträgen geregelt) sorgen dafür, daß dies mit den Zielen der Kunden vereinbar ist. Allgemein bekannt sind solche Systeme unter dem Namen Continuous Replenishment, das beispielsweise der Großhändler Wal-Mart bereits implementiert hat (vgl. [19]).

Entwicklungsstufe 4

Ein Information Broker führt nach Bedarf Unternehmen und Einzelpersonen mit den notwendigen Kernkompetenzen zusammen, um gezielt eine Marktaufgabe zu erfüllen. Als Motivation einer solchen Veränderung der Organisationsstruktur (bis hin zu ihrer Auflösung) dienen einerseits die Erwartung einer verkürzten Time-to-Market und andererseits neue Möglichkeiten, die aus verbesserten IKS entstehen: „Thanks to new technologies, executives can divide up their companies’ value chains, handle the key strategic elements internally, outsource others advantageously, any-where in the world with minimal transaction costs, and yet coordinate all essential activities more effectively to meet customers’ needs.“ [33]. Die Entwicklungsstufe 4 in Abbildung 3 weicht leicht vom Modell-VU aus Kapitel 2.2 ab. Ein Widerspruch besteht aber deshalb nicht, weil es von der Marktaufgabe abhängt, ob die Koordination im VU allein von IKS wahrgenommen werden kann, oder ob ein Information Broker bzw. ein Leader-Unternehmen auftritt, der bzw. das diese Funktion zusätzlich unterstützt (vgl. 34]). Das am häufigsten aufgeführte Beispiel für diese Stufe ist die Rosenbluth International Alliance [35], illustrierend dafür ist aber auch die IBM-Tochtergesellschaft AMBRA.

Ein weiteres Beispiel ist Lewis Galoob Toys (vgl. [36], S. 3): Dieser US-amerikanische „Hersteller“ von Spielwaren, beschäftigt kaum mehr als 100 fest angestellte Mitarbeiter und vermarktet Waren im Wert von über 50 Mio. \$ (1985). Galoob kauft Produktideen von unabhängigen Erfindern und läßt die Entwicklungsarbeit von selbständigen Ingenieurbüros durchführen. Die eigentliche Herstellung erfolgt durch Subkontrakt-Unternehmen

in Hongkong, die ihrerseits arbeitsintensive Funktionen in China ausführen (lassen). Die Fertigprodukte werden durch Spediteure in den USA transportiert und dort über selbständige Vertragsrepräsentanten vertrieben. Selbst Funktionen wie Factoring und Finanzbuchhaltung werden von selbständigen Dienstleistungsunternehmen ausgeführt. Galoob beschränkt sich im Kern auf die strategische Führung dieses Netzwerkes selbständiger Unternehmen, tritt also als Leader-Firma auf. Noch vor wenigen Jahren wurde Galoob von einigen Beobachtern als „[...] very alien business creature“ [37, S. 243] angesehen. In der Zwischenzeit ist das Modell aber bereits von einigen Konkurrenten erfolgreich adaptiert worden.

9.1.9 Enterprise-on-demand

9.2 Beispiele

9.2.1 Amazon.com (oder ähnlich)

9.2.2 parts.com (oder ähnlich)

9.2.3 MyWorld (oder ähnlich)

Für anonyme Lottospieler - Jaxx-Lottokiosk **Fehler! Verweisquelle konnte nicht gefunden werden.**]

9.2.4 Virtueller Lebensmitteleinkauf

Ein aktueller Trend im B2C-Bereich sind virtuelle Supermärkte. Diese bestehen aus einem riesigen Zentrallager, einem Shop-Server sowie einem Lieferdienst. Über den Shop-Server können Lebensmittel ausgewählt und bestellt werden. Nun sind Lebensmittel nicht immer gleich Lebensmittel – einige sind intensiv zu befehlen, bevor man sie in den realen Einkaufswagen legt. Folglich reduziert sich das Online-Angebot eher auf „Commodities“, also Gebrauchsgüter mit minimalem Spezifikationsaufwand, z.B.

- Eier der Güteklasse A,
- Ein Kasten Bier,
- Ein 400-Gramm-Glas Nutella etc.

Auch hierbei besteht noch kein echter Vorteil des minutenlangen Shop-Surfens gegenüber der ebenfalls minutenlangen Hatz durch die Supermarktregale. Spannend wird es erst, wenn ein Prozeß eingerichtet werden kann, der dem des Supply-Chain-Management entspricht. Wie kann also ein privates Kanban-System (der richtige

Artikel zum richtigen Zeitpunkt am richtigen Ort) installiert werden, das für alle Beteiligten vorteilhaft ist. Die wichtigsten Anforderungen sind dabei:

- Kostenreduktion oder zumindest nur moderate Mehrkosten
- Reduzierte Lagerhaltung
- Minimierung der Transportkosten
- Minimierung der Anzahl an Lieferungen
- Keine zusätzlichen Umstände für den Käufer durch die Lieferung

Man stelle sich vor: Die Eier sind im wöchentlichen Rhythmus, das Glas Nutella im monatlichen zu liefern. Während des 2-wöchigen Urlaubs ist keine Lieferung erforderlich und wenn Freunde für eine Woche zu Besuch sind, erhöht sich der Bierkonsum. Weder will man die Ware selbst beim Supermarkt abholen (dann könnte man gleich die weiteren 10 Minuten für den Einkauf spendieren), noch sie sich um 11.30 nach Hause liefern lassen (dann sitzt man nämlich im Büro). Auch das Wochenende ist unpassend, da man ungern die persönliche Zeitplanung von der Nutella-Lieferung abhängig machen möchte. Schließlich möchte man nicht mehrmals wöchentlich von einem Lieferanten belästigt werden – es könnte ja sein, daß man auch einmal ins Kino gehen will. Wir stellen fest, daß wir uns auf widrigem Terrain bewegen, denn am Ende soll dieser Prozeß ja für den Händler profitabel und für den Konsumenten in irgendeiner Form nutzbringend sein.

Interessanter wird die Situation sicherlich, wenn man sich Nischenmärkte ansieht: Bringdienste versorgen ältere Personen bereits heute mit Tiefkühlkost und warmen Mahlzeiten und beispielsweise ist der Nutzen in Skandinavien, wo die Entfernungen zum Supermarkt erheblich größer sind, offensichtlich: In Norwegen verkauft das Unternehmen *REMA 1000* seit Anfang 1998 Lebensmittel über das Internet. Aus fünf speziell dafür eingerichteten Lagern wird innerhalb von zwei Stunden geliefert. Die Lieferung selbst kostet 50 norweg. Kronen (XXX DM?). Der monatliche Umsatz soll etwa 25 Mio norweg. Kronen betragen (<http://www.rema.no/>). Auch in der Schweiz gibt es einen Internet-Supermarkt "LeShop" (<http://www.leshop.ch>). Bezahlt wird mit der Kreditkarte, die Lieferung erfolgt für 9,- Franken (ca. 11,- DM).

In Deutschland entstehen ebenfalls diverse Lieferdienste:

Das *Einkaufsnetz* ist unter <http://www.einkaufsnetz.de> zu erreichen. Geliefert wird überall im Stadtgebiet von XXX Hamburg??? solange die Bestellung zwischen 8.30 und 13 Uhr eingeht. Ab 16 Uhr wird die Ware nach Hause geliefert. Der Mindestbestellwert liegt bei 40,- Mark zzgl. einer Lieferpauschale von 5,- DM. Außerdem bietet in Hamburg eine Gemüsehändlerin ihre Naturkost online an: <http://www.naturkost-express.de>.

Bei CityWeb (<http://www.cityweb.de>) bietet die Reichelt AG unter der Rubrik "City Market". im CityMarket Berlin unter "Essen & Trinken" eine Service für den virtuellen Lebensmitteleinkauf an. Der Mindestbestellwert liegt bei DM 30,-. Zusätzlich fallen DM 10,- an Lieferkosten an. Diese entfallen bei einem Warenwert ab DM 150,-. Bezahlt wird in Bar oder per Scheck bei der Lieferung vor Ort.

Nach diesen "Early Birds" beginnen nun jedoch auch die "Großen", sich mit diesem Marktsegment zu befassen. Der weltweit zweitgrößte Handelskonzern Metro AG (Umsatz 1997: 64 Milliarden Mark) arbeitet an einer Lösung für den Internet-Vertrieb seiner Lebensmittel. Ca. 7000 Artikel wird dieses System umfassen und dem Kunden die Ware noch am selben Tag ins Haus liefern. Dabei ist jedoch zu bedenken, daß Metro-Kunden im Food-Bereich in der Regel Wiederverkäufer oder auch Restaurantbesitzer sind. Deren monatlicher übersteigt den der Kleinfamilie um Größenordnungen, so daß die on-demand-Auslieferung sich eher rechnen könnte.

Der Internet-Lebensmittelservice ist Teil einer strategischen Online-Orientierung. Im Sommer 1998 hat Metro ihren Online-Dienst "Metronet" umstrukturiert, ist eine Kooperation mit dem Daimler-Benz-Systemhaus Debis eingegangen und ein gemeinsames Tochterunternehmen *Primus Online* gegründet. Für die Online-Aktivitäten im Lebensmittelbereich stand ein Startbudget von 100 Millionen DM bereit.

Aber nicht nur bei der Metro als der deutschen Nummer eins, auch bei der Nummer zwei (Karstadt AG) werden Waren online geliefert: Mit MyWorld ist Karstadt bereits seit Jahren im Mall-Geschäft etabliert. Es ist eine Frage der Zeit, bis auch hier Gedanken zum Thema "Virtueller Lebensmitteleinkauf" öffentlich werden, da auch Supermarktketten wie XXX zum Karstadt-Konzern zählen.

9.2.5 Online-Kauf von Briefmarken

Was ist eigentlich eine Briefmarke? Eigentlich ist sie mit einer Münze vergleichbar, die wir auf einen Brief kleben können. Von der Post wird sie jedoch entwertet, wenn der Brief bei der Verteilzentrale ankommt. Mit der

Eigenschaft als Münze gehen alle Bargeld-Eigenschaften einher, es ist daher keine besonders waghalsige Überlegung, elektronische Bargeldsysteme wie Ecash o. ä. zu diesem Zweck einzusetzen. Einfacher noch: die Briefmarke wird nicht zwischen drei Parteien (Bank, Kunde, Händler) ausgetauscht, sondern nur zwischen zwei (Post und Kunde). Die wichtigsten Anforderungen sind dabei:

- Fälschungssicherheit. Dies kann durch Verwenden einer Seriennummer und Speichers des Hash-Wertes der Briefmarken-Daten seitens der Post erfolgen. Wird die Marke "eingereicht", kann erkannt werden, ob ihr Hash-Wert vorhanden ist (dann ist sie gültig). Wenn der Hash-Wert bereits einmal benutzt wurde, liegt ein Double-Spending vor.
- Überwindung des Medienbruchs Digital-Papier. Hier bietet sich ein Barcode als Papier-Repräsentation an. Der Kunde könnte den Barcode zum Beispiel zusammen mit der Postanschrift des Adressaten auf den Umschlag Drucken, so daß nicht für jede Briefmarke Endlospapier mit Aufklebern in den Drucker eingelegt werden braucht.
- Flexible Gebühreneinheiten. Im Gegensatz zur umständlichen Quantisierung der Markeneinheiten, könnten Briefmarken jetzt exakt proportional zum Gewicht des Briefes generiert werden (also z.B. 1,45 DM für 67,5 Gramm).
- Eine Intranet-Infrastruktur zur Zusammenschaltung der Ausgabe- und Verifikationssoftware und ihren Datenbanken. Dies umfaßt eine komplexe Infrastruktur vom Barcode-Scanner über kryptographische Verfahren bis zur Finanzbuchhaltung
- Anonymität. Dies ist sicherlich ein wichtiges Kundeninteresse, allerdings kann die Post anhand der Absender und Adressateninformation bereits heute erkennen, wen an wen was versendet. Durch den Einsatz blind geleisteter Unterschriften (siehe Ecash im Abschnitt XXX) steht ein Mechanismus zur Verfügung der nicht nur Anonymität sondern auch über Erweiterungen des Verfahrens das Aufdecken mehrfach verwendeter Briefmarken aufdeckt.
- Abrechnung. Das die Postzustellung heute noch monopolistisch erfolgt und auch für die Zukunft zu erwarten ist, daß ein einzelner Kunde nur zwischen wenigen Anbieter aussuchen kann, ist davon auszugehen, daß das Einrichten eines Gebührenkontos am Markt akzeptiert wird. Damit sind nun Briefmarken nicht mehr einzeln zu erwerben, sondern man kann sich ein Konto einrichten lassen, von dem die Markenbeträge abgebucht werden.

Interessant ist hier vor allem der Einsatz von SmartCards, da diese mit einem Guthabenbetrag von der Post aufgeladen werden können, das Abbuchen der Markengebühr erfolgt dann über die Zugriffsfunktionen eines Smart-Card-Lesegerätes. Eine besonders interessante Anwendung ist hier die Nutzung des Java-Rings der Firma iButton. Der Java-Ring besitzt die Logik einer SmartCard und dient dem Träger zur Authentisierung sowie als Speicher von Wertmarken.

9.2.6 Music-on-Demand

9.2.7 Elektronische Notare

Nachdem wir den umfangreichen Komplex der kryptographischen Grundlagen sowie der Zertifizierungsinfrastruktur bewältigt haben, sind noch einige weitere Mechanismen und Dienste zu behandeln, die ebenfalls einer vertrauenswürdigen Kommunikation auf dem elektronischen Markt dienen. Diese sind

- Nichtabstreitbarkeits-Dienste (im folgenden auch Notariatsdienste genannt) sowie
- Versicherungsdienste (nächster Abschnitt) und
- Vertragsdienste (nächster Abschnitt).

Das Angriffspotential liegt ohne Notare auf der Ebene von Teilnehmerbeziehungen in der Behauptung eine Handlung durchgeführt oder eben nicht durchgeführt zu haben – jeweils unwissend oder in bössartiger Absicht, jedoch im Widerspruch zur tatsächlichen Handlung. Beispiele sind etwa

- Die Behauptung eine Zahlung durchgeführt zu haben, ohne tatsächlich bezahlt zu haben

- Die Behauptung keine Bezahlung empfangen zu haben, obwohl diese tatsächlich eingetroffen ist.

Das Problem der Nichtabstreitbarkeit entspricht dem des Einschlebens im täglichen Leben. Nur wenn ein vertrauenswürdiger Dritter (der Postbote) das Schreiben dem Empfänger persönlich übergibt, dabei die Identität der Person feststellt und sich den Empfang schriftlich bestätigen läßt, kann davon ausgegangen werden, daß ein Zugang tatsächlich erfolgt ist. Wird der Brief nur in den Briefkasten geworfen, oder an irgendeine, sich im Haushalt befindliche Person übergeben, besteht bereits Abstreitbarkeitspotential für die Person (oder eher ihren juristisch gewandten Rechtsanwalt...).

Umgesetzt in die Technik des Internet, ist es schwierig, Nichtabstreitbarkeit wirklich zu erreichen. Schließlich ist es nie die Person des Empfängers, die eine Nachricht entgegennimmt und betätigt, sondern ihre Software. Es ist ein schwieriges Unterfangen, zu behaupten, eine e-Mail nicht empfangen zu haben, auch wenn sie eingetroffen ist, aber wie ist der Sachverhalt, wenn zufälligerweise (oder aus anderen Gründen) doch der betreffende Rechner gerade zum falschen Zeitpunkt abstürzte (schließlich nutzen e-Mail-Server keine verteilten Transaktionsprotokolle).

Unter der Voraussetzung, daß derartige, äußerst seltene Extremfälle außer acht gelassen werden können, und damit mit einer Empfangsbestätigung der Anwendungssoftware gerechnet werden kann, macht die Einschaltung eines elektronischen Notars Sinn, der den Datenaustausch zwischen den beiden Parteien burkundet.

9.3 Wohin führt Electronic Commerce

Internet-Handel: überschätzt und unterschätzt **Fehler! Verweisquelle konnte nicht gefunden werden.**]

Was wird sich ändern?

10 Ausblick

2-3 Seiten

XXX

11 Index

A

Anonymität

uneingeschränkte · 61

B

Börsensystem · 112

D

Dienstangebotsverwaltung · 111

Diensttyp

Definition · 111

E

Ecash

Protokoll · 61

M

Münzen

elektronische · 61

S

Schnittstellentyp · 111

12 Literatur

- [12] CEC project AC206 ABS, Project Deliverable D23: Broker business model. See <http://b5www.berkom.de/ABS/>, October 1996
- [TINA95] TINA Consortium. „Overall Concepts and Principles of TINA“. Version 1.0. February, 1995.
- [TINA97] TINA Consortium. „TINA Business Model and Reference Points“. Version 4.0. May, 1997
- [ITU95] ITU-T X.901 ODP Reference Model Part 1 Overview and guide to use of the Reference Model, November 1995.
- [ATAK97] E. Athanassiou, I. Tothezan, P. Alzon and G. T. Karetsos. „Enterprise Modelling of Information Brokerage and Retailer Services“. *First international enterprise distributed object computing workshop (EDOC'97)*. Marriott Resort, Gold Coast, Australia. October 1997.
- [LMNE94] Lai C., Medvinsky G., Neuman B.C, Endorsements, Licensing, and Insurance for Distributed System Services, Proceedings of the 2nd ACM Conference on Computer and Communications Security, November 1994.
- [2] Object Management Group. „Electronic Commerce DTF Reference Model“. *OMG document ec/96-09-02*. September, 1996.
- [3] ITU-T Recommendation X.903. „Information technology - Open distributed processing - Reference model: Architecture“. 1995.
- [4] Enterprise Modeling: Practices and Perspectives, Lars Chr. Christensen, Brage W. Johansen, Nils Midjo, Jan Onarheim, Tor G. Syvertsen and Terje Totland. Proceedings of ASME Ninth Engineering Database Symposium, Boston, MA, September 1995.
- [4] UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport), EDIFACT Syntax Rules (ISO 9735) and EDIFACT Data Element Directory (ISO 7372), 1993.
- [5] ITU-T X.900 series: Open Distributed Processing Reference Model (ODP-RM), November 1995
- [5] Crocker D., MIME Encapsulation of EDI Objects, RFC 1767 of the IETF EDI Working Group, March 1995.
- [6] ETSI/SRC6 report on the European Information Infrastructure, part B.2, 21 June 1995.
- [6] Bons R., Lee R., Wagenaar R., Wrigley C., Computer Aided Design of Interorganisational Trade Scenarios, A CASE for Open-edi, Report. no. WP 94.03.01, Erasmus University Research Institute for Decision and Information Systems (EURIDIS), March 1994.
- [7] ISO TC 184 SC5 WG1: Draft International Standard 14528: Industrial automation systems Concepts and rules for enterprise models, 15 January 1997.
- [7] ISO/IEC JTC/WG3, The Open-EDI Reference Model, Working Draft document N255, 1994.
- [8] Bruce T. Krulwich, An Agent of Change. See <http://bf.cstar.ac.com/bf/>
- [8] Milosevic Z., Berry A., Bond A., Raymond K., Supporting Business Contracts in Open Distributed Systems, the 2nd International Workshop on Services in Distributed and Networked Environments (SDNE'95), Whistler, Canada, June 1995.
- [9] Sara Record, Personalized Electronic Information Service. See <http://www.infosage.ibm.com/>
- [BöRi98] K. Böhle und U. Riehm: „Blütenträume - Über Zahlungssysteminnovationen und Internet-Handel in Deutschland.“, <http://www.itas.fzk.de/deu/PROJEKT/pez.htm>
- [CCITT89] Empfehlung X.509, "The Directory-Authentication Framework", CCITT, Genf 1989
- [Dres98] Stephan Dresen, Thomas Dunne: Fürs Netz geprägt iX 4/98 S. 110 1998

- [Escher97] Markus Escher: Bankrechtsfragen des elektronischen Geldes im Internet. WM Wertpapier-Mitteilungen. Zeitschrift für Wirtschafts- und Bankrecht 51(1997)25, S.1173-1220 bzw. <http://www.gassner.de/e-geld-txt.htm>
- [EU98] Europäische Kommission: „Vorschlag für die EU Directive zum Elektronischen Handel“: COM(1998) 586
- [Fran98] Georg Franck: „Ökonomie der Aufmerksamkeit“. München: Hanser 1998
- [Gentz97] Wolfgang Gentz: „Die elektronische Geldbörse in Deutschland: Funktionsweise, Kosten und Nutzen für die Beteiligten“. Diplomarbeit, Fachhochschule München, 1997
- [GiLe98] O. Giarini, P. M. Liedtke: „Wie wir arbeiten werden“, Hoffmann und Campe, Hamburg, 1998
- [Gold98] Michael H. Goldhaber: „Die Aufmerksamkeitsökonomie und das Netz - Teil II“. <http://www.heise.de/tp/deutsch/inhalt/eco/6200/1.html>
- [KrGo98] M. Krüger und H. Godschalk: „Herausforderung des bestehenden Geldsystems im Zuge seiner Digitalisierung - Chancen für Innovation?“ Gutachten der PaySys GmbH, <http://www.itas.fzk.de/deu/PROJEKT/pez.htm>
- [LeDr92] Lee, R.M., Dewitz, S.D., Facilitating International Contracting: AI Extensions to EDI, International Information Systems, January 1992.
- [MML95a] M. Merz, K. Müller, W. Lamersdorf : *Electronic Market Support for the Tourism Industry: Requirements and Architectures*, in: W. Schertler, B. Schmid/A M. Tjoa/ H. Werthner (Hrsg.): Proc. ENTER95, Springer-Verlag, Wien New York, (1995), S. 220ff
- [MML95b] K. Müller-Jones, M. Merz, W. Lamersdorf: *The TRADER Integrating Trading into DCE* in: J. de Meer, B. Reynolds, J. Slonim (Hrsg.): Proc. ICODP, Chapman Hall 1995
- [MML95c] M. Merz, K. Müller-Jones, W. Lamersdorf: *Mobile Klienten: Ortsübergreifender Zugang zu Diensten in offenen verteilten Informationssystemen*, Proc. GI/SI Jahrestagung, ETH Zürich, (1995)
- [MML95d] K. Müller-Jones, M. Merz, W. Lamersdorf: *Realisierung von Kooperationsanwendungen auf der Basis erweiterter Diensttypbeschreibungen* , in: H. Krumm (Hrsg.), Entwicklung und Management verteilter Anwendungssysteme, Krehl Verlag, Münster 1995
- [Schu98] Lutz Schumacher: Geldgeschäfte Internet World 5/98 S. 42 1998
- [SDKL+94] M. Stonebraker, R. Devine, M. Kornacker W. Litwin, A. Pfeffer, A. Sah, C. Staelinet al.: "An Economic Paradigm for Query Processing and Data Migration in Mariposa", Sequoia 2000 Technical Report 94/49, University of California, Berkeley, CA, Apr. 1994. Auch erschienen in: *Proceedings of 3rd International Conference on Parallel and Distributed Information Systems*, Austin, TX, USA, 28-30 Sept. 1994. Los Alamitos, CA, USA: IEEE Comput. Soc. Press, 1994. p. 58-67.
- [Wrig91] Wright B., The Law of Electronic Commerce, EDI, Fax and E-Mail: Technology, Proof, and Liability, Little Brown and Company, 1991
- [ScFE97] Schuster R., Färber J., Eberl M: DigitalCash. Springer Verlag Berlin Heidelberg 1997
- [Esch99] Escher, Markus: Aktuelle Rechtsfragen des Zahlungsverkehrs im Internet, in: Lehmann, Michael (Hrsg.), Rechtsgeschäfte im Netz - Electronic Commerce, Schäffer-Poeschel-Verlag 1999, Seite 225 ff.
- [ApBe98] W. Appel, R. Behr: *Towards the theory of Virtual Organisations: A description of their formation and figure*. In: virtual-organisation.net Newsletter, Vol 2(2), 1998.
- [BiBS98] M. Bichler, C. Beam, A. Segev: A Broker-Centered Object Framework for Electronic Requisitioning. In: W. Lamersdorf, M. Merz (Hrsg.): Proc. TREC'98 Intl. Conference on Trends in Distributed Systems for Electronic Commerce, Springer LNCS 1402, S. 154-165

- [BJ95] A. Bertsch, M. Jurecic: *Notariatsdienste zum nachweisbaren Austausch personenbezogener Daten*. In: P. Horster (Hrg.): Trust Center. DuD Fachbeiträge, 1995.
- [ByBP93] J. A. Byrne, R. Brandt, O. Port: *The Virtual Corporation*. In: Business Week, 8. Februar 1993, S. 36-40.
- [ChMa96] A. Chavez and P. Maes. "Kasbah: An Agent Marketplace for Buying and Selling Goods." In: Proc. of the First International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology. London, UK, April 1996.
- [CommerceNet99] CommerceNet: *eCo Framework Project*.
<http://www.commerce.net/projects/currentprojects/eco/index.htm>, 1999.
- [COSMOS99] COSMOS: *Project Home Page*. [Http://www.ponton-hamburg.de/cosmos](http://www.ponton-hamburg.de/cosmos), 1999.
- [CSTAR96] CSTAR (Andersen Consulting): The BargainFinder agent: Comparison price shopping on the Internet. In J. Williams (ed.): Bots and Other Internet Beasities, SAMS.NET publishing, 1996.
http://www.ac.com/services/cstar/cstar_child/ecagents_cn.html.
- [DISA98] Data Interchange Standards Association. <http://www.disa.org>, 1998.
- [Entropolis99] Entropolis HomePage: <http://www.entropolis.de/>
- [EU95/46] Amtsblatt der Europäischen Gemeinschaften (Nr. L 281 vom 23. November 1995 S. 31)
- [EU98] EU: *European Initiative in Electronic Commerce*.
<http://www.ispo.cec.be/ecommerce/initiat.htm>, 1998.
- [FW96] A. Furche, G. Wrightson: *Computer Money : A Systematic Overview of Electronic Payment Systems*. Morgan Kaufman Publishers, 1996.
- [GP98] C. Goldfarb, P. Prescod: *The XML Handbook*. Prentice Hall, 1998.
- [Grif98] F. Griffel: *Componentware - Konzepte und Techniken eines Softwareparadigmas*. dpunkt, 1998.
- [HaBi93] V. Hammer, J. Bizer: *Beweiswert elektronisch signierter Dokumente*. In: Datenschutz und Datensicherung (DuD) 12/93, S.689-699.
- [IBM98] IBM: SanFrancisco product information. <http://www.ibm.com/Java/Sanfrancisco/technical.html>, 1998.
- [Intershop99] Intershop. <http://www.intershop.com>, 1999.
- [ISO94] ISO/IEC: *Information Technology - Open Systems Interconnection - Data Management and Open Distributed Processing - Basic Reference Model of Open Distributed Processing*. ISO Dokument Nr. ISO/IEC DIS 10746, 1994.
- [ISO95] ISO/IEC: *Trading Function Specification*. ISO Dokument Nr. ISO/IEC 13235, 1995.
- [ISO97] ISO: *ODP Trader Specification*. ISO/IEC IS 13235-1, ITU/T Draft Rec X950-1, Part 1, 1997
- [Jens92] K. Jensen: *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use*. Springer 1992.
- [KF98] M. Kumar, F. Feldman: *Business negotiations on the Internet*. IAC Reports, IBM Research Division, T.J. Watson Research Center, <http://www.ibm.com/iac>, 1998.
- [LaMe98] Lamersdorf, M. Merz (Hrsg): *Trends in Distributed Systems for Electronic Commerce*. Lecture Notes in Computer Science, vol. 1402, Springer-Verlag, Berlin Heidelberg New York, 1998.
- [MeLL97] M. Merz, B. Liberman, W. Lamersdorf: *Using Mobile Agents to Support Interorganizational Workflow-Management*. In: International Journal on Applied Artificial Intelligence, 11(6), September 1997, S. 551ff.
- [Merz99-1] M. Merz: *Elektronische Handelstransaktionen im Internet: Modelle und Methoden des Electronic Commerce*. Springer-Verlag, Heidelberg, New York, erscheint 1999.
- [Merz99-2] M. Merz: *Electronic Commerce*. dpunkt, Heidelberg, 1999.

- [MGBW+99] M. Merz, F. Griffel, M. Boger, H. Weinreich, W. Lamersdorf: *Electronic Contracting im Internet*. In: R. Steinmetz, L. Wolf (Hrsg.): GI/ITG-Konferenz „Kommunikation in Verteilten Systemen“ (KiVS'99), Informatik-Aktuell, Springer-Verlag, 1999.
- [MGTM+98] M. Merz, F. Griffel, T. Tu, S. Müller-Wilken et al.: *Supporting Electronic Commerce Transactions with Contracting Services*. In: International Journal on Cooperative Information Systems, 4(7), Dezember 1998, S. 1-25.
- [MiAC96] Z. Milosevic, D. Arnold, L. O'Connor: *Inter-enterprise Contract Architecture For Open Distributed Systems: Security Requirements*. WET ICE'96 Workshop on Enterprise Security, Stanford, USA, June 1996.
- [Milo95] Z. Milosevic: *Enterprise Aspects Of Open Distributed Systems*“. PhD. Thesis, Department of Computer Science, University of Queensland, 1995.
- [MJML95] K. Müller-Jones, M. Merz, and W. Lamersdorf, *Kooperationsanwendungen: Integrierte Vorgangskontrolle und Dienstvermittlung in offenen verteilten Systemen*. In: F. Huber-Wäschle, H. Schauer, and P. Widmayer, eds., GISI 95 - Herausforderungen eines globalen Informationsverbundes für die Informatik, Zurich, pp. 518-525, Springer 1995.
- [MMM97] S. McConnell, M. Merz, L. Maesano, and M. Witthaut: *An open architecture for electronic commerce*. OMG/ECDTF/OSM Response, 1997.
- [Mondex98] Mondex USA. <http://www.mondexusa.com>, 1998.
- [MultiMed99] MultiMediator Project Homepage: <http://www.cselt.stet.it/sonah/MULTIMEDIATOR>
- [Netscape98a] Netscape, Firefly, Verisign: *Open Profiling Standard (OPS)*. <http://developer.netscape.com/ops/ops.html>, 1998.
- [Netscape98b] Netscape: *Secure Sockets Layer*. <http://www.netscape.com/products/security/ssl/index.html>, 1998.
- [OMG93] Object Management Group: "The Common Object Request Broker: Architecture and Specification". Specification 1.2, Framingham, Ma., USA, OMG Document No. 91.12.1, 1993
- [OMG96] AT&T, DSTC, DEC, HP, ICL, Nortel, and Novell: *Trading Object Service*. OMG Dokument Nr.: orbos/96-05-06, Version 1.0, 1996.
- [OMG98] Object Management Group: *CORBA BOCA - Business Object Component Architecture*". OMG Dokument Nr. bom/98-01-07, 1998.
- [OpenMarket99] Open Market: *LiveCommerce*. <http://www.openmarket.com/livecom>, 1999.
- [OPT97] D. O'Mahony, M. Peirce, H. Tewari: *Electronic Payment Systems*. Artech House, 1997.
- [Oracle99] Oracle. <http://www.oracle.com>, 1999.
- [OTP98] Open Trading Protocol Consortium. <http://www.otp.org>, 1998.
- [Schm95] B. Schmid et al.: *Electronic Mall: Banking und Shopping in globalen Netzen*. Teubner, Stuttgart 1995.
- [Schn95] B. Schneier: *Applied Cryptography: Protocols, Algorithms, and Source Code in C*". John Wiley & Sons, 1995.
- [ShBD98] G. Shamir, M. Ben-Or, D. Dolev: BARTER: A Backbone Architecture for Trade of Electronic Content. In: W. Lamersdorf, M. Merz (Hrsg.): Proc. TREC'98 Intl. Conference on Trends in Distributed Systems for Electronic Commerce, Springer LNCS 1402, S. 65-79
- [Sieber98] P. Sieber: *Virtuelle Unternehmen in der IT-Branche*. Berner betriebswirtschaftliche Schriften, Band 19, Haupt Verlag, 1998.
- [SSS97] B. Schmid, D. Selz, R. Sing (eds.): *Electronic Product Catalogs*. EM - Electronic Markets, Vol. 7, No. 3. http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/717, 1997.

- [Sun98] Sun Micro Systems: *Java Commerce Homepage*.
<http://www.javasoft.com/products/commerce/index.html>, 1999.
- [TGML98] T. Tu, F. Griffel, M. Merz, W. Lamersdorf: *A Plug-in Architecture Providing Dynamic Negotiation Capabilities for Mobile Agents*. In: Proc. 2. Intl. Workshop on Mobile Agents, MA'98, Stuttgart, 1998, Springer LNCS, S. 222-236.
- [TINA98] The TINA Consortium: *TINA-C technical library*. <http://www.tinac.com>, 1998.
- [W3C98] World Wide Web Consortium: *Platform for Privacy Preferences (P3P) Project*.
<http://www.w3.org/P3P>, 1998.
- [Webe98] R. Weber: Chablis - "Market Analysis of Digital Payment Systems". Version 1.0. TU München, Technical Report TUM-I9819, 18. August 1998
- [WoJe94] M.J. Wooldridge, N.R. Jennings: "Agent Theories, Architectures, and Languages: A Survey". In: M.L. Woolridge, N.R. Jennings, Hrsg., *Intelligent Agents*, Springer, 1994 S. 1-39
- [AFHS95] O. Arnold, W. Faisst, M. Härtling, P. Sieber: "Virtuelle Unternehmen als Unternehmenstyp der Zukunft?". In: HMD – Handbuch der Datenverarbeitung, Vol. 32, Ausgabe 185, 1995, S. 8-22
- [Crai97] A. Craig: „SAP, Digital Try to Eliminate Empty Vending Machines“. Internet Week, November 1997. Auch: <http://www.techweb.com/se/directlink.cgi?INW19971103S0027>
- Internet Micropayment Protocols, Chris A. Owen
- [Ponton-Lino-Presserklärung]

The State of the Art in Electronic Payment Systems; Asokan N., Janson P.A., Steiner M. Weidner M.

13 URLS

13.1 Electronic Commerce Allgemein

Business Software Alliance – Prinzipien des ECommerce: <http://www.bsa.org/ceoforum/pdfs/ecommerce.pdf>

American Bar Association <http://www.abanet.org/buslaw/efss>

Australian Electronic Transactions Bill exposure draft <http://law.gov.au/ecommerce/>

[Weltbank97] Bericht der Weltbank „Rethinking the State“
<http://www.worldbank.org/html/extpb/wdr97/english/wdr97su1.htm>

Ein ABC für Electronic Commerce findet sich unter der URL <http://www.electronic-commerce.org/abc/index.htm>.

[ScZi97] B. Schmid, H.-D. Zimmermann: „Eine Architektur Elektronischer Märkte auf der Basis eines generischen Konzeptes für elektronische Produktkataloge“, White Paper, Information Multimedia Communications GmbH 4/97, November 1997

13.2 Sicherheit und Vertrauen

Cheskin Research study on **building trust in e-Commerce** <http://www.studioarchetype.com/cheskin/>

SmartCards

Informationen zu SmartCards

PC/SC Workgroup: www.smartcardsys.com

Opencard: www.opencard.org

JavaCard Forum: www.javacardforum.org

Sun: java.sun.com/products/javacard

iButton: www.ibutton.com

IBM: www.chipcard.ibm.com

Gemplus: www.gemplus.com

Schlumberger: www.slb.com/et

Paul Kocher und seine Angriffe gegen die Sicherheit von SmartCards:

--> Der Artikel aus der New York Times findet sich auch hier:

<http://www.jya.com/dpa-news2.htm>.

--> Weitere Informationen zum DPA-Verfahren gibt es hier:

<http://www.cryptography.com/dpa>.

--> Paul Kochers Unternehmen Cryptography Research in San Francisco hat die Homepage <http://www.cryptography.com>.

Paul Kocher ist bereits 1995 durch seine "Timing Attack" bekannt geworden. Er konnte nachweisen, daß der geheime Schlüssel im Public Key Verfahren durch Zeitmessungen der kryptographischen Operationen (z.B. auf einer Chipkarte oder einem PC) entschlüsselt werden konnte. Siehe:

<http://www.cryptography.com/timingattack/paper.html>.

Datenschutz

Department of Commerce press release: US and EU moving closer on data protection issues
<http://www.usia.gov/current/news/latest/99020503.clt.html?/>

European Commission Data Protection Working Party opinion on the level of data protection in the U.S.

<http://www.privacyexchange.org/news/990129wpdoc.html>

13.3 Zahlungsverfahren

Zahlungsverfahren Allgemein

Übersichten zu Internet-Zahlungsverfahren:

Federal Reserve Bank of New York - Überblick zu Zahlungssystemen: <http://www.ny.frb.org/bankinfo/payments/>

<http://medoc.informatik.tu-muenchen.de/Chablis/MStudy/>

<http://www.electronic-commerce.org/zahlungssysteme/>

Micropayment-Standardisierung beim WWW Consortium: <http://www.w3.org/ECommerce/Micropayments/>

overview page <http://www.w3.org/ECommerce/Micropayments/Overview.html>

http://www.hrl.il.ibm.com/mpay/sub_registry.html

SET

<http://www.mastercard.com/>

<http://www.visa.com/>

<http://www.terisa.com/>

SET-Erfahrungsberichte: <http://www.ecin.de/zahlungssysteme/set1.htm>

Geldkarte

<http://www.gdm.de/>

CyberCash

<http://www.cybercash.de>, <http://www.cyberash.com>

<http://www.cybercash.com/>

<http://www.dresdner-bank.de/>

Ecash

<http://www.digicash.com/>

<http://www.digicash.com/ecash/docs/works/>

MilliCent

<http://www.millicent.com/>

NetBill

<http://www.ini.cmu.edu/netbill/>

<http://www.netbill.com/>

Mini-Pay

http://www.ibm.net.il/ibm_il/int-lab/mpay/

Weitere Zahlungsverfahren

Lottery Tickets, PayWord, MicroMint: <http://theory.lcs.mit.edu/~rivest/publications.html>

Announcement of **DigiGold** electronic currency system: <http://www.digigold.net/DigiGoldPressRelease.html>

Aktivitaeten der Financial Issues Working Group FIWG der EU zu **SmartEuro:**
<http://www.ispo.cec.be/fiwg/smartgen.htm>

Informationen zu UCC – Uniform Commercial Code <http://www.law.upenn.edu/library/ulc/ucc2/ucc2299.htm>

American Bar Association Business Law Section Commercial Financial Services and UCC Committees
<http://www.abanet.org/buslaw/cfs-ucc/home.html>

Department of Commerce and FTC press release on growth of online shopping and importance of consumer protection <http://204.193.243.2/public.nsf/docs/commerce-ftc-press-release>

PayCard der Telekom

Auf die Schnelle einige Links zur PayCard fuer eine erste Basisinformation.

<http://www.telekom.de/aktuell/presse/archiv/0828975.htm>

<http://www.vdv.de/vdvappl/presse4.htm>

<http://www.vdv.de/vdvappl/presse22.htm>

<http://www.online.de/home/Telefonkarte/paycard.htm>

<http://homes.cls.net/~clino/Telekom/T-Card.htm>

Politisches

Australian Electronic Transactions Bill exposure draft: <http://law.gov.au/ecommerce/>

Studie der EU Kommission zum praktizierten Datenschutz in ausgewählten Geschäftsbereichen
<http://europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.htm>

Financial Information Privacy Act of 1999, introduced by Senators Sarbanes, Dodd and Leahy
<http://thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c10628p8G2>

Statement of SEC Chairman Levitt re risks of online trading <http://www.sec.gov/news/levonlin.htm>

NASDAQ press release on trading in turbulent markets http://www.nasdaq-amexnews.com/news/pr99/ne_section99_17.html

BOLERO initiative on electronic trade documentation <http://www.bolerold.com/index.htm>

Global Business Dialogue on Electronic Commerce <http://www.gbde.org/>

Peter Troberg: Elektronische Zahlungssysteme. Was geschieht auf EG-Ebene?
<http://www.itas.fzk.de/deu/tadn/tadn298/trob298a.htm>

Interview mit Charles Goldfinger: „At the Coal-face Between Financial Industries and Politics“
<http://www.itas.fzk.de/deu/tadn/tadn298/gold298a.htm>

Elektronische Verträge

Allen and Widdison "Can Computers Make Contracts": <http://www.dur.ac.uk/Law/centre/hjolt.html>

13.4 Online-Shopping

<http://www.netzmarkt.de>

<http://www.my-world.de>

<http://www.quelle.de>

<http://www.shopping24.de>

IVW-Webstatistik (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V.)
<http://www.ivw.de/data/index.phtml>

Nähere Informationen zu den durchgeführten Befragungen zu **Junk-Orders** finden sich Übrigens in der erwähnten Studie:

GMD Research Series Nr.2 / 1998

Internet-Shopping heute

Nähere Infos siehe

<http://wsv.gmd.de/aiv/series.htm>

Online-Rating Agenturen

--> Internet Intern Ausgabe 18/98 (3.9.98) <http://www.intern.de/98/18/14.shtml>

--> Bizrate hat die URL <http://www.bizrate.com> und der Betreiber von Bizrate <http://www.binarycompass.com>

--> Shop.de findet sich unter <http://www.shop.de> und dessen Betreiber unter <http://www.berensp.com>

Unbekannter Inhalt

<http://www.zurich.ibm.com/Technology/Security/publications/>

<http://www.zurich.ibm.com/Technology/Security/extern/tutorial/10.96/tutorial.pdf>

<http://www.zurich.ibm.com/Technology/Security/extern/tutorial/9.97/061-088.pdf>

<http://www.zurich.ibm.com/Technology/Security/extern/tutorial/4.95/tutorial.pdf>

EDI

Premenos

<http://www.cals.com/edi/>

<http://www2.echo.lu/oii/en/edi.html>

<http://www2.echo.lu/oii/en/payguide.html> (hier werden auch OFX, etc,erläutert)

ICE

Informastionen zu ICE: <http://www.w3.org/TR/NOTE-ice>

Elektronische Verträge

Surf^oN^oSign: Benutzersignaturen auf Web-Dokumenten, by A. Herzberg and D. Naor

<http://www.almaden.ibm.com/journal/sj/371/herzberg.html>

13.5 Sonstiges

Liste deutscher ISPs Unter <http://www.heise.de/ct/provider>

FATF-Bericht (Financial Action Task Force) vom 12.2. "1997-1998 REPORT on MONEY LAUNDERING TYPOLOGIES" <http://www.oecd.org/fatf/fatfix.htm>

IDA-Projekt zum Thema A2A-Commerce: <http://www.ispo.cec.be/ida/idahome.htm>