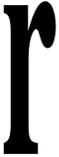


Martin Manninger, Karl Michael Göschka,
Christian Schwaiger, Dietmar Dietrich

Electronic Commerce - Die Technik

Technologie, Design und Implementierung



Inhaltsverzeichnis

1	Einleitung: Information, Kommunikation und Wirtschaft	1
2	Veränderte Rahmenbedingungen	16
2.1	Architekturen und Begriffsbestimmungen	16
2.1.1	Definition von Electronic Commerce	16
2.1.2	Handlungsrollen und Geschäftsmodelle	18
2.1.3	Waren und Kommunikationsnetze	20
2.1.4	Transaktionsphasen	21
2.1.5	Bedeutung des Internets und Netzwerkexternalitäten	22
2.2	Business to Consumer Commerce	23
2.2.1	Ablauf einer typischen Geschäftstransaktion	23
2.2.2	Käufer im B2C-Commerce	23
2.2.2.1	Informationssuche	26
2.2.2.2	Nutzen des B2C-Commerce für die Kunden	29
2.2.3	Verkäufer im B2C-Commerce	31
2.2.3.1	Online-Shops und Mails	33
2.2.3.2	Marketing und Kundenbindung	38
2.2.4	Privacy	41
2.3	Business to Business Commerce	42
2.3.1	Standards, Protokolle und Szenarien für den Datenaustausch	43
2.3.2	Intermediäre	47
2.4	Politisches Umfeld des EC	52
2.4.1	Maßnahmen der EU	54
2.4.2	Standpunkt der USA	58
3	Basistechnologien	61
3.1	Grundlagen: Internet, Web und Software Engineering	62
3.1.1	Aufbau und Dienste des Internet	62
3.1.1.1	Überblick über die TCP/IP-Protokollfamilie	63
3.1.1.2	IP und ARP	64
3.1.1.3	TCP, UDP, ICMP und Sockets	64
3.1.1.4	DNS	65
3.1.2	World Wide Web	66
3.1.2.1	Hypertext Markup Language HTML	66

3.1.2.2	Uniform Resource Locator.....	68
3.1.2.3	Das Hypertext Transfer Protocol.....	69
3.1.2.4	Common Gateway Interface.....	71
3.1.2.5	JavaScript - ECMA Script.....	71
3.1.3	Software Engineering und Web Engineering.....	72
3.1.4	Java.....	73
3.2	Client/Server und Schichtenmodelle.....	78
3.2.1	Datenbanken und Wissensbanken.....	78
3.2.1.1	Relationale Datenbanken.....	79
3.2.1.2	Objektorientierte und objektrelationale Datenbanken.....	79
3.2.1.3	Weitere Datenbanksysteme.....	80
3.2.1.4	Directory Services.....	81
3.2.2	Client/Server- und N-Schichten-Architekturen.....	83
3.2.3	Objektorientierung und Persistenz.....	85
3.2.3.1	Objekt-Serialisierung.....	87
3.2.3.2	Spezifische Persistenz.....	88
3.2.3.3	Gekapselter Datenbankzugriff.....	88
3.2.3.4	Persistenz-Frameworks.....	89
3.2.3.5	Orthogonale Persistenz in objektorientierten Datenbanken.....	90
3.2.4	Integration des Schichtenmodells mit den Persistenzansätzen.....	91
3.3	Flexible und heterogene Clients.....	92
3.3.1	HTML Client.....	92
3.3.1.1	User Interface: HTML und ECMA Script.....	92
3.3.1.2	Protokoll: Probleme mit HTTP.....	93
3.3.1.3	Verbindung von Web-Server und Middleware: CGI und API.....	94
3.3.2	Java-Applets.....	95
3.3.3	Vergleich von Java-Applets und reinem HTML.....	95
3.3.4	Java-Applikation.....	98
3.3.4.1	Applikation mit Netzwerk-ClassLoader.....	98
3.3.4.2	Vollständige Applikation am Client.....	99
3.3.5	Andere Programmiersprachen als Java am Client.....	100
3.3.6	Applikation und Datenbank am Client.....	100
3.3.7	Client am Mobiltelefon: WAP und WML.....	101
3.3.7.1	WAP-Protokoll-Stack.....	101
3.3.7.2	Wireless Markup Language WML.....	104
3.3.7.3	WML Scripting Language.....	105
3.3.8	Virtual Reality Modeling Language VRML.....	105
3.4	Verteilte Systeme und Middleware.....	107
3.4.1	Anforderungen an die Middleware.....	108
3.4.2	CORBA.....	110
3.4.2.1	Grundstruktur und Object Request Broker.....	110
3.4.2.2	Interface Definition Language IDL.....	112
3.4.2.3	Bedeutung der Object-Adapter.....	114
3.4.2.4	CORBA Messaging.....	115
3.4.2.5	Auffinden von verteilten Objekten.....	116

3.4.2.6	Weitere CORBA-Dienste.....	118
3.4.2.7	Zusammenfassung und Bewertung von CORBA.....	119
3.4.3	Java am Application-Server.....	120
3.4.3.1	Remote Method Invocation RMI.....	120
3.4.3.2	Servlets.....	121
3.4.3.3	Datenbankzugriff mit Java: JDBC und SQLJ.....	122
3.4.3.4	Enterprise JavaBeans.....	123
3.4.3.5	Java Cryptography Architecture JCA.....	125
3.4.4	Distributed Component Object Model DCOM.....	125
3.4.5	Transaktionssicherheit.....	127
3.4.6	Architekturkonzepte für die horizontale Verteilung.....	129
3.4.6.1	Web-Clients mit verteilter Middleware.....	130
3.4.6.2	Web-basierte Client/Server-Architektur.....	131
3.4.6.3	Objektorientiertes, verteiltes System.....	131
3.4.6.4	Objektorientierte 3-Tier-Architektur.....	132
3.4.6.5	Web-basierte 3-Tier-Architektur.....	132
3.4.7	Application-Server und Object Request Broker.....	133
3.4.7.1	Oracle Application Server.....	133
3.4.7.2	Orbix.....	134
3.4.7.3	VisiBroker von Inprise.....	134
3.4.7.4	Voyager.....	135
3.4.7.5	Orbit.....	135
3.4.7.6	OmniORB2.....	135
3.4.7.7	IBM WebSphere Application-Server.....	136
3.4.7.8	Netscape Application-Server.....	136
3.4.7.9	Microsoft Transaction-Server.....	136
3.5	Plattformunabhängige Daten.....	136
3.5.1	Extensible Markup Language XML.....	137
3.5.2	Praktischer Umgang mit XML und Java.....	138
3.5.3	XML-Strukturen und Navigation.....	140
3.5.3.1	XML Namespaces.....	140
3.5.3.2	XML Linking: XPointer und XPath.....	140
3.5.3.3	Style Sheets für XML.....	142
3.5.3.4	Schema und Data Binding.....	143
3.5.4	XML als Interface Definition Language.....	144
3.5.5	Electronic Data Interchange.....	144
3.6	Zukunftstrends.....	145
3.6.1	Software-Agents.....	145
3.6.1.1	Agent-Schnittstellen.....	145
3.6.1.2	Virtuelle Marktplätze.....	146
4	Sicherheitsmechanismen.....	148
4.1	Sicherheit.....	148
4.1.1	Sicherheitsbegriffe.....	148
4.1.1.1	Grundbedrohungen.....	149

4.1.1.2	Kryptografie.....	150
4.1.1.3	Kryptoanalyse.....	151
4.1.2	Basismechanismen der Kryptografie.....	152
4.1.2.1	Einwegfunktionen, Falltüren und Hash-Werte.....	152
4.1.2.2	Symmetrische Verschlüsselungsverfahren.....	153
4.1.2.3	Asymmetrische Verschlüsselungsverfahren.....	155
4.1.2.4	Digitale Signaturen, Zertifikate und MACs.....	156
4.1.2.5	Authentifizierung und Autorisierung.....	158
4.1.2.6	Beurteilung kryptografischer Verfahren.....	160
4.1.3	Sicherheit und Evaluierung.....	163
4.2	Chipkarten.....	172
4.2.1	Typen von Chipkarten.....	172
4.2.2	Chipkarten-Normen.....	174
4.2.3	Funktionsweise von Chipkarten.....	175
4.2.3.1	Dateisystem der Smart Card.....	176
4.2.3.2	Kommunikation zwischen Chipkarte und Terminal.....	177
4.2.3.3	Genormte Kommandos für Smart Cards.....	178
4.2.4	Sicherheitsaspekte bei Chipkarten.....	179
4.2.4.1	Hardware-Sicherheitsmaßnahmen.....	179
4.2.4.2	Software-Sicherheitsmaßnahmen.....	179
4.2.4.3	Erfolgreiche Angriffe.....	181
4.2.5	Elektronische Geldbörsen.....	182
4.2.5.1	Quick.....	182
4.2.5.2	Andere Geldbörsen.....	184
4.2.6	Harmonisierung.....	185
4.3	Internet und Sicherheit.....	186
4.3.1	Bekannte Sicherheitslücken.....	186
4.3.1.1	Klartextübertragung, insbesondere inLANs.....	186
4.3.1.2	IPspoofing.....	186
4.3.1.3	DNSSpoofing.....	187
4.3.2	Internet-Sicherheitsmechanismen.....	187
4.3.2.1	Firewalls.....	188
4.3.2.2	SSL.....	190
4.3.2.3	S-HTTP.....	191
4.3.2.4	PGP.....	191
4.3.2.5	PEMundX.509.....	193
4.3.2.6	S/MIME.....	195
4.4	Netzwerksicherheit durch Chipkarten.....	195
4.4.1	Angriffspunkte.....	195
4.4.2	Absicherung verteilter Systeme.....	197
4.4.3	Schlüssel- und Rechteverwaltung.....	198
5	Zahlungsverkehr: Cybermoney.....	199
5.1	Cybermoney-Theorie.....	199
5.1.1	Begriffsdefinitionen.....	199

5.1.2	Anforderungen an Cybermoney.....	202
5.2	Varianten von Cybermoney.....	206
5.2.1	PayNow.....	207
5.2.2	SET.....	209
5.2.3	First Virtual.....	210
5.2.4	E-Gold.....	212
5.2.5	NetCash.....	212
5.2.6	eCash.....	214
5.2.7	eCoin.....	215
5.3	Smart-Card-Cybermoney.....	217
5.3.1	Funktionalität.....	217
5.3.2	Portabilität.....	219
5.3.3	Verteilung der Intelligenz zwischen Client und Server.....	220
5.3.4	Ablauflogik und deren Einfluss auf Funktionalität und Benutzeroberfläche.....	220
5.3.4.1	Aktivität des Clients.....	221
5.3.4.2	Aktivität des Servers.....	222
5.3.5	Parallele Transaktionen.....	223
5.3.6	Hängende Transaktionen.....	225
5.3.7	Maximierung der Sicherheit.....	226
5.3.7.1	Sicherheit der elektronischen Geldbörse.....	226
5.3.7.2	Hinzukommende Angriffsmöglichkeiten durch das Internet.....	226
5.3.7.3	Absicherung des Smart-Card-Cybermoney.....	229
5.3.8	Eigenschaften des Smart-Card-Cybermoney.....	234
6	E-Commerce in der Praxis.....	236
6.1	Ticketverkauf der Österreichischen Bundesbahnen.....	237
6.1.1	Architekturen für das Ticketverkaufssystem.....	238
6.1.2	Clients.....	240
6.1.2.1	Internet-Client.....	240
6.1.2.2	Reisebüro-Client.....	240
6.1.2.3	Kassen-Client.....	241
6.1.2.4	Zwischenlösung Kassen-Client.....	241
6.1.2.5	Automaten-Client.....	242
6.1.3	Middleware-Architektur.....	242
6.1.3.1	Integration neuer Module.....	242
6.1.3.2	Serverarchitektur für die Internetlösung.....	242
6.1.4	Erste Erfahrungen mit WAP und WML.....	244
6.1.5	Erste Erfahrungen mit Software-Agents.....	246
6.1.6	Bewertung.....	247
6.2	DEMENET - das DEMETER-Projekt.....	248
6.3	Open and Distance Learning.....	253
6.4	Kreditkarten-Transaktionen im Internet (SET).....	254
6.4.1	Händler-Software.....	254

6.4.2 Kunden-Software.....	257
6.4.3 Kryptografische Absicherung von SET.....	259
6.5 Tele-Banking mit HBCL.....	260
7 Ausblick und Resümee.....	266
Abkürzungsverzeichnis.....	277
Literaturverzeichnis.....	282
Stichwortverzeichnis.....	301