

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

# **E- und M-Commerce - Die Technik**

**Technologie, Design und Implementierung**

2., neu bearbeitete und erweiterte Auflage

Hüthig Verlag Heidelberg

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung.....</b>	<b>1</b>
1.1	Wirtschaftliche Entwicklung des E-Commerce.....	2
1.2	Technische Entwicklung.....	6
<b>2</b>	<b>Veränderte Rahmenbedingungen.....</b>	<b>12</b>
2.1	Architekturen und Begriffsbestimmungen.....	12
2.1.1	Definition von Electronic Commerce.....	12
2.1.2	Handlungsrollen und Geschäftsmodelle.....	14
2.1.3	Waren und Kommunikationsnetze.....	15
2.1.4	Transaktionsphasen.....	16
2.1.5	Bedeutung des Internets und Netzwerkexternalitäten.....	17
2.2	Business to Consumer Commerce.....	18
2.2.1	Ablauf einer typischen Geschäftstransaktion.....	18
2.2.2	Käufer im B2C-Commerce.....	19
2.2.2.1	Informationssuche.....	22
2.2.2.2	Nutzen des B2C-Commerce für die Kunden.....	25
2.2.3	Verkäufer im B2C-Commerce.....	27
2.2.3.1	Online-Shops und Mails.....	28
2.2.3.2	Marketing und Kundenbindung.....	33
2.2.4	Privacy.....	35
2.3	Business to Business Commerce.....	37
2.3.1	Standards, Protokolle und Szenarien für den Datenaustausch.....	37
2.3.2	Intermediäre.....	41
2.4	Politisches Umfeld des EC.....	45
2.4.1	Maßnahmen der EU.....	49
2.4.2	Standpunkt der USA.....	53
<b>3</b>	<b>Basistechnologien.....</b>	<b>55</b>
3.1	Grundlagen: Internet, Web und Software Engineering.....	56
3.1.1	Aufbau und Dienste des Internets.....	56
3.1.1.1	Überblick über die TCP/IP-Protokollfamilie.....	57
3.1.1.2	IPundARP.....	58
3.1.1.3	TCP, UDP, ICMP und Sockets.....	58
3.1.1.4	DNS.....	59
3.1.1.5	FTP, SMTP und POP.....	60
3.1.2	World Wide Web.....	60
3.1.2.1	Hypertext Markup Language: HTML und XHTML.....	61
3.1.2.2	Uniform Resource Locator.....	63
3.1.2.3	Das Hypertext Transfer Protocol.....	63
3.1.2.4	Common Gateway Interface.....	65
3.1.2.5	Scripting: JavaScript - ECMA Script und VBScript.....	66

3.1.3	Software Engineering und Web Engineering.....	67
3.1.4	Grundlagen von Java.....	68
3.2	Schichtenmodelle, Verteilte Systeme und Komponenten.....	72
3.2.1	Datenbanken und Wissensbanken.....	73
3.2.1.1	Relationale Datenbanken.....	74
3.2.1.2	Objektorientierte und objektrelationale Datenbanken.....	74
3.2.1.3	Weitere Datenbanksysteme.....	75
3.2.1.4	Directory Services.....	76
3.2.2	Client/Server- und N-Schichten-Architekturen.....	77
3.2.3	Objektorientierung und Persistenz.....	81
3.2.3.1	Objekt-Serialisierung.....	83
3.2.3.2	Spezifische Persistenz.....	84
3.2.3.3	Gekapselter Datenbankzugriff.....	85
3.2.3.4	Persistenz-Frameworks.....	86
3.2.3.5	Orthogonale Persistenz in objektorientierten Datenbanken.....	87
3.2.4	Integration des Schichtenmodells mit den Persistenzansätzen.....	87
3.2.5	Transaktionssicherheit.....	88
3.2.6	Verteilte Systeme.....	90
3.2.7	Anforderungen an die Middleware.....	94
3.2.8	Komponentensysteme.....	95
3.2.8.1	Warum CBSE?.....	97
3.2.8.2	Produktion und Integration von Komponenten.....	98
3.2.8.3	Definitionen.....	98
3.2.8.4	Komponentenmodelle und Komponentenservices.....	105
3.2.9	Konzepte für die horizontale Verteilung.....	112
3.3	Plattformen: Standards und Technologien.....	114
3.3.1	CORBA.....	114
3.3.1.1	Grundstruktur und Object Request Broker.....	117
3.3.1.2	Interface Definition Language IDL.....	120
3.3.1.3	Bedeutung der Object-Adapter.....	128
3.3.1.4	Interface Repository, Dynamic Invocation Interface und Dynamic Skeleton Interface.....	131
3.3.1.5	CORBA Messaging.....	133
3.3.1.6	CORBA Services: Überblick über die Objektdienste.....	135
3.3.1.7	Auffinden von verteilten Objekten: Naming und Trading Service ..	137
3.3.1.8	Event Service.....	140
3.3.1.9	Notification Service.....	142
3.3.1.10	Transaction Service und Concurrency Control Service.....	143
3.3.1.11	Persistent State Service.....	146
3.3.1.12	CORBA Component Model.....	149
3.3.1.13	Zusammenfassung und Bewertung von CORBA.....	155
3.3.2	Enterprise Java.....	156
3.3.2.1	Java Messaging Service JMS.....	157
3.3.2.2	Remote Method Invocation RMI.....	157
3.3.2.3	Datenbankzugriff mit Java: JDBC und SQLJ.....	160
3.3.2.4	JavaBeans.....	161
3.3.2.5	Enterprise Java Beans - Grundlagen und Konzept.....	162

3.3.2.6	EJB-Architektur.....	162
3.3.2.7	EJB-Rollenkonzept.....	168
3.3.2.8	EJB-Transaktionskonzept.....	170
3.3.2.9	EJB-Persistenzkonzept.....	170
3.3.2.10	Integration von Java und CORBA.....	171
3.3.3	Component Object Model COM+.....	171
3.3.3.1	Die Microsoft IDL und die Systemregistrierung als Interface Repository.....	173
3.3.3.2	Kommunikation und Lokalisierung: DCOM.....	176
3.3.3.3	COM+im Detail.....	182
3.3.3.4	IMoniker-Intelligent Name Service.....	186
3.3.3.5	COM+Ereignisdienst.....	187
3.3.3.6	Distributed Transaction Coordinator (DTC).....	189
3.3.3.7	IPersist und IStorage - Persistenz in COM+.....	190
3.3.3.8	ActiveX.....	192
3.3.3.9	.NET.....	193
3.3.4	Zusammenfassung und Vergleich.....	193
3.3.4.1	Vergleich RMI - CORBA IIOP.....	194
3.3.4.2	Vergleich der Komponentenmodelle COM+, EJB und CCM.....	195
3.3.4.3	Migrationsaspekte und Legacy Integration.....	200
3.3.4.4	Produkte und Referenzen .....	200
3.4	Flexible und heterogene Clients für B2C.....	201
3.4.1	HTML-Client und Web-Server-Anbindung.....	202
3.4.1.1	User Interface: HTML und ECMA Script.....	T.203
3.4.1.2	Protokoll: Probleme mit HTTP.....	203
3.4.1.3	Verbindung von Web-Server und Middleware: CGI und API.....	205
3.4.1.4	Servlets und Java Server Pages.....	205
3.4.2	Java-Applets.....	208
3.4.3	Vergleich von Java-Applets und reinem HTML.....	209
3.4.4	Non-Web Clients.....	212
3.4.4.1	Java-Applikation.....	213
3.4.4.2	Andere Programmiersprachen als Java auf dem Client.....	214
3.4.4.3	Applikation und Datenbank auf dem Client.....	214
3.4.4.4	GUI Frameworks und generische Ansätze.....	215
3.4.5	Mobile Devices und Sprach-/Datenkonvergenz.....	215
3.4.5.1	Clients am Mobiltelefon: WAP und WML.....	216
3.4.5.2	WAP-Protokoll-Stack.....	217
3.4.5.3	Wireless Markup Language WML.....	219
3.4.5.4	WML Scripting Language.....	220
3.4.6	Virtual Reality Modeling Language VRML.....	220
3.5	XML und Web Services für B2B.....	222
3.5.1	eXtensible Markup Language XML.....	223
3.5.1.1	XML-Grundkonzepte: „well formed“ und „valid“.....	223
3.5.1.2	XML-Strukturen und Navigation: Namespaces und Linking.....	225
3.5.1.3	Darstellung von XML: Style Sheets und XSLT.....	227
3.5.1.4	Zugriff auf XML: SAX und DOM.....	228
3.5.1.5	XML Schema und Data Binding.....	230

3.5.1.6	XML als Interface Definition Language.....	232
3.5.2	Plattformunabhängige Daten: EDI und XML.....	233
3.5.2.1	Vom Papier über EDI zu XML.....	233
3.5.2.2	Electronic Data Interchange.....	234
3.5.2.3	XML im E-Commerce.....	235
3.5.3	Web Services.....	236
3.5.3.1	Die Architektur von Web Services.....	236
3.5.3.2	Die Web Service Description Language WSDL.....	239
3.5.3.3	Das Simple Object Access Protocol SOAP.....	242
<b>4</b>	<b>Sicherheitstechnologien.....</b>	<b>245</b>
4.1	Sicherheit.....	245
4.1.1	Sicherheitsbegriffe.....	245
4.1.1.1	Grundbedrohungen.....	246
4.1.1.2	Kryptografie.....	248
4.1.1.3	Kryptoanalyse.....	248
4.1.2	Basismechanismen der Kryptografie.....	249
4.1.2.1	Einwegfunktionen, Falltüren und Hash-Werte.....	249
4.1.2.2	Symmetrische Verschlüsselungsverfahren.....	250
4.1.2.3	Asymmetrische Verschlüsselungsverfahren.....	253
4.1.2.4	Digitale Signaturen, Zertifikate, PKI und MACs.....	254
4.1.2.5	Authentifizierung und Autorisierung.....	257
4.1.2.6	Zufallszahlen.....	259
4.1.3	Beurteilung kryptografischer Verfahren.....	261
4.1.4	Sicherheit und Evaluierung.....	264
4.2	Chipkarten.....	273
4.2.1	Typen von Chipkarten.....	273
4.2.2	Chipkarten-Normen.....	275
4.2.3	Funktionsweise von Chipkarten.....	276
4.2.3.1	Dateisystem der Smart Card.....	279
4.2.3.2	Kommunikation zwischen Chipkarte und Terminal.....	279
4.2.3.3	Genormte Kommandos für Smart Cards.....	281
4.2.4	Sicherheitsaspekte bei Chipkarten.....	282
4.2.4.1	Hardware-Sicherheitsmaßnahmen.....	282
4.2.4.2	Software-Sicherheitsmaßnahmen.....	282
4.2.4.3	Erfolgreiche Angriffe 1996 - 2000.....	284
4.2.5	Chipkarten für den Zahlungsverkehr.....	285
4.2.5.1	Debit- und Kreditkarten nach EMV-Standard.....	286
4.2.5.2	Elektronische Geldbörsen.....	288
4.2.6	Chipkarten für die Mobiltelefonie.....	290
4.2.6.1	SIM-Karten.....	291
4.2.6.2	USIM-Karten.....	295
4.3	Internet und Sicherheit.....	295
4.3.1	Bekannte Sicherheitslücken.....	295
4.3.1.1	Klartextübertragung, insbesondere in LANs.....	295
4.3.1.2	IPspoofing.....	296
4.3.1.3	DNSSpoofing.....	297

4.3.2	Internet-Sicherheitsmechanismen.....	297
4.3.2.1	Firewalls.....	298
4.3.2.2	Intrusion Detection Systems (IDS).....	299
4.3.2.3	VPNs mit PPTP, L2F und L2TP.....	302
4.3.2.4	SSLundTLS.....	303
4.3.2.5	SSH.....	305
4.3.2.6	S-HTTP.....	306
4.3.2.7	PGP.....	307
4.3.2.8	PEM.....	309
4.3.2.9	S/MIME und PGP/MIME.....	309
4.3.3	Netzwerksicherheit durch Chipkarten.....	310
4.3.3.1	Angriffspunkte.....	310
4.3.3.2	Absicherung verteilter Systeme.....	312
4.3.3.3	Schlüssel- und Rechteverwaltung.....	313
4.4	Mobiltelefonie und Sicherheit.....	313
4.4.1	GSM-Sicherheit.....	314
4.4.2	UMTS-Sicherheit.....	317
<b>5</b>	<b>Elektronisches Geld: Cybermoney.....</b>	<b>321</b>
5.1	Cybermoney-Theorie.....	321
5.1.1	Begriffsdefinitionen.....	321
5.1.2	Europäische Richtlinien.....	324
5.1.3	Anforderungen an Cybermoney.....	325
5.2	Varianten von Cybermoney.....	328
5.2.1	Einweg-Kreditkartennummern.....	331
5.2.2	PayNow.....	332
5.2.3	Paybox.....	334
5.2.4	SET.....	335
5.2.5	First Virtual.....	340
5.2.6	E-Gold.....	342
5.2.7	PayPal.....	343
5.2.8	Paysafecard.....	344
5.2.9	NetCash.....	345
5.2.10	eCash.....	347
5.2.11	eCoin.....	348
5.2.12	Elektronische Geldbörsen.....	349
5.2.13	Sicheres M-Payment mit SIM.....	352
<b>6</b>	<b>E-Commerce in der Praxis.....</b>	<b>355</b>
6.1	Ticketverkauf der Österreichischen Bundesbahnen.....	356
6.1.1	Architekturen für das Ticketverkaufssystem.....	357
6.1.2	Clients.....	359
6.1.2.1	Internet-Client.....	359
6.1.2.2	Reisebüro-Client.....	359
6.1.2.3	Kassen-Client.....	360
6.1.2.4	Zwischenlösung Kassen-Client.....	360
6.1.2.5	Automaten-Client.....	360
6.1.3	Middleware-Architektur.....	361

6.1.3.1	Integration neuer Module.....	361
6.1.3.2	Serverarchitektur für die Internetlösung.....	361
6.1.4	Erste Erfahrungen mit WAP und WML.....	363
6.1.5	Bewertung.....	365
6.1.6	Die Umsetzung des Konzeptes.....	366
6.2	Open and Distance Learning.....	368
6.3	Quick im Internet.....	369
6.3.1	Funktionalität.....	369
6.3.2	Portabilität.....	370
6.3.3	Verteilung der Intelligenz zwischen Client und Server.....	371
6.3.4	Ablauflogik und deren Einfluss auf Funktionalität und Benutzeroberfläche.....	372
6.3.4.1	Aktivität des Clients.....	372
6.3.4.2	Aktivität des Servers.....	373
6.3.5	Parallele Transaktionen.....	375
6.3.6	Hängende Transaktionen.....	376
6.3.7	Maximierung der Sicherheit.....	377
6.3.7.1	Sicherheit der elektronischen Geldbörse.....	377
6.3.7.2	Hinzukommende Angriffsmöglichkeiten durch das Internet.....	377
6.3.7.3	Absicherung des Smart-Card-Cybermoney.....	380
6.3.8	Kommerzielle Implementierung.....	385
6.4	Tele-Banking mit HBCI.....	385
<b>7</b>	<b>Ausblick und Resümee.....</b>	<b>391</b>
	<b>Abkürzungsverzeichnis.....</b>	<b>397</b>
	<b>Literaturverzeichnis.....</b>	<b>406</b>
	<b>Stichwortverzeichnis.....</b>	<b>429</b>