

TATA MCGRAW-HILL EDITION

Web Commerce Technology Handbook

Secure Electronic Transaction

Internet EDI

Digital Signatures

Daniel Minoli • Emma Minoli

Contents

Part 1 Overview

Chapter 1 Electronic Commerce Environment and Opportunities	3
1.1 Background	3
1.1.1 Basic Web Commerce Concepts	6
1.1.2 Scope of This Text	12
1.2 The Electronic Commerce Environment	12
1.2.1 The Virtual Corporation	12
1.2.2 The Electronic Marketers	16
1.2.3 The Catalyst of Electronic and Web Commerce	17
1.2.4 Available Communication Apparatus	20
1.2.5 Applications of Electronic/Web Commerce	24
1.2.6 Benefits of Electronic/Web Commerce	28
1.2.7 Elements of a Successful Electronic Marketplace	31
1.2.8 Security Issues and Approaches Related to Web Commerce	35
1.2.9 Size of Electronic Marketplace	43
1.3 Electronic Marketplace Technologies	45
1.3.1 Electronic Data Interchange	45
1.3.2 On-line Networks and Services	45
1.3.3 The Internet: Web Commerce	47
1.3.4 CD-ROMs and Hybrids	49
1.3.5 Screen Phones	51
1.3.6 Kiosks	52
1.3.7 Interactive Television and Video Dial Tone	52
1.3.8 WebTV	54
1.3.9 Interactive Banking	56
1.4 Conclusion	56
References	57
Chapter 2 Modes of Electronic Commerce	61
2.1 Overview	62
2.1.1 What Is Electronic Commerce?	62
2.1.2 Some Open Issues	64

2.2	Electronic Data Interchange	
2.2.1	What Is EDI?	64
2.2.2	EDI's Benefits	64
2.2.3	Status	67
2.2.4	System Approach	69
2.2.5	Communication Approach	70
2.3	Migration to Open EDI	71
2.3.1	Approach	73
2.3.2	Benefits	73
2.3.3	Mechanics	75
2.3.4	Challenges	76
2.3.5	Examples	77
2.4	Electronic Commerce with WWW/Internet	78
2.4.1	Opportunities	78
2.4.2	Internet/Web Statistics	81
2.4.3	Internet and WWW Tools	87
2.5	CommerceNet Advocacy	89
2.6	Web Commerce Going Forward	95
	References	98
		99

Chapter 3 Approaches to Safe Electronic Commerce

3.1	Overview	101
3.2	Secure Transport Protocols	101
3.2.1	S-HTTP	107
3.2.2	SSL	108
3.2.3	Alternatives	108
3.3	Secure Transactions	109
3.4	Secure Electronic Payment Protocol (SEPP)	110
3.4.1	SEPP Process	112
3.4.2	SEPP Architecture	112
3.5	Secure Electronic Transaction (SET)	116
3.6	Certificates for Authentication	118
3.7	Security on Web Servers and Enterprise Networks	122
3.7.1	Host Security Considerations	123
3.7.2	Enterprise Network Security	124
3.8	Conclusion	133
	References	141
		142

Chapter 4 Electronic Cash and Electronic Payment Schemes

4.1	Internet Monetary Payment and Security Requirements	145
4.1.1	Confidentiality of Payment Information	146
4.1.2	Payment Information Integrity	148
4.1.3	Account holder and Merchant Authentication	150
4.1.4	Interoperability	150
4.2	Payment and Purchase Order Process	151
4.2.1	Overview	151
4.2.2	Account Holder Registration	151
4.2.3	Merchant Registration	153
4.2.4	Account Holder (Customer) Ordering	153
4.2.5	Payment Authorization	156

4.3	On-line Electronic Cash	156
4.3.1	Overview	157
4.3.2	Problems with Simple Electronic Cash	157
4.3.3	Creating Electronic Cash Anonymity	157
4.3.4	Preventing Double-Spending	159
4.3.5	E-Cash Interoperability	160
4.3.6	Electronic Payment Schemes	160
	References	174

Part 2 Security

Chapter 5	Internet/Intranet Security Issues and Solutions	179
5.1	The Need for Computer Security	179
5.1.1	Reasons for Information Security	181
5.1.2	Protecting Resources	184
5.1.3	Types of Risks	185
5.2	Specific Intruder Approaches	189
5.2.1	Bulletin Boards	189
5.2.2	Electronic mail	190
5.2.3	File Transfer	190
5.2.4	IP Spoofing	190
5.2.5	Password Guessing	190
5.2.6	Password Sniffing	191
5.2.7	Telnet	191
5.2.8	Viruses	191
5.2.9	SATAN	192
5.3	Security Strategies	192
5.3.1	Policy Issues	195
5.3.2	Mechanisms For Internet Security	202
5.4	Security Tools	202
5.4.1	Secure Transport Stacks	203
5.4.2	Kerberos	206
5.4.3	Secure Transactions over the Internet	206
5.4.4	UNIX Security	207
5.4.5	Password Security Systems	209
5.4.6	Electronic Mail	212
5.4.7	Server Security	212
5.4.8	Trusting Binaries	213
5.5	Encryption	216
5.5.1	Conventional Encryption	217
5.5.2	Public-Key Encryption	219
5.5.3	Application of Encryption	221
5.5.4	Breaking an Encryption Scheme	222
5.5.5	The Data Encryption Standard	223
5.5.6	Commercial Communications Security Endorsement Program	223
5.5.7	Government Security Levels	225
5.5.8	The Clipper Chip	225
5.5.9	Commercial Outlook on Encryption	228
5.6	Enterprise Networking and Access to the Internet	229
5.6.1	Approaches for Enterprise-Level Security	234
5.6.2	Variations and Combinations	236
5.6.3	Design Considerations	236

5.7	Antivirus Programs	242
5.7.1	Viruses and Worms	242
5.7.2	The Nature of Viruses	243
5.7.3	Countering the Threat of Viruses	243
5.8	Security Teams	244
5.8.1	Computer Emergency Response Team (CERT)	244
5.8.2	Forum of Incident Response and Security Teams (FIRST)	244
	Glossary	245
	References	248
 Chapter 6 MasterCard/Visa Secure Electronic Transaction		251
6.1	Introduction	252
6.1.1	Background	252
6.1.2	Objectives	254
6.2	Business Requirements	256
6.2.1	Requirements	256
6.2.2	Features	257
6.2.3	Scope	259
6.3	Concepts	261
6.3.1	Payment System Participants	261
6.3.2	Cryptography	262
6.3.3	Certificate Issuance	270
6.3.4	Kinds of Shopping	273
6.4	Payment Processing	275
6.4.1	Overview	275
6.4.2	Cardholder Registration	276
6.4.3	Merchant Registration	287
6.4.4	Purchase Request	294
6.4.5	Payment Authorization	301
6.4.6	Payment Capture	305
6.4.7	Additional Messages	309
 Chapter 7 E-mail and Secure E-mail Technologies for Electronic Commerce		311
7.1	Introduction	311
7.2	The Means of Distribution	314
7.3	A Model for Message Handling	315
7.3.1	ITU-T Model	315
7.3.2	Internet Apparatus	317
7.4	How Does E-mail Work?	318
7.4.1	UUEncode/UUDecode	321
7.5	MIME: Multipurpose Internet Mail Extensions	322
7.5.1	Basic Concepts	322
7.5.2	MIME Body Parts	327
7.5.3	MIME Data Encoding Techniques	331
7.5.4	Address Directory	332
7.6	S/MIME: Secure Multipurpose Internet Mail Extensions	332
7.7	MOSS: Message Object Security Services	332
7.7.1	Purpose	335
7.7.2	MOSS Services—Overview	335
7.7.3	Definition of Security Subtypes	336
		340

7.7.4 Application of MIME Object Security Services	343
7.7.5 Pretty Good Privacy (PGP)	346
7.8 Comparisons of Security Methods	349
7.9 MIME and Related Facilities for EDI over the Internet	349
References	353

Part 3 Internet and Web Site Establishment

Chapter 8 Internet Resources for Commerce 359

8.1 Introduction	359
8.1.1 Commercialization of the Internet	360
8.1.2 The Web Breakthrough	363
8.1.3 How to Connect to the Internet	367
8.1.4 Browsers	368
8.2 Technologies for Web Servers	371
8.2.1 HTML	371
8.2.2 Data Collection	375
8.2.3 Publishing Systems	376
8.3 Internet Tools Relevant to Commerce	382
8.3.1 Archie	382
8.3.2 File Transfer Protocol	383
8.3.3 Gopher	383
8.3.4 Telnet	383
8.3.5 Veronica	384
8.3.6 WAIS	384
8.3.7 Usenet Newsgroups	384
8.3.8 Other Internet Applications	384
8.4 Internet Applications for Commerce	385
8.4.1 Direct Selling	387
8.4.2 Selling Ad Space	388
8.4.3 Charging for Content	388
8.4.4 Charging for Services	388
8.5 Internet Charges	388
8.5.1 Browsing for Information	389
8.5.2 Browsing and Providing Information	390
8.5.3 Settlements	393
8.6 Internet Access and Architecture	394
8.6.1 Routing Arbiters (RAs)	395
8.6.2 Example of NAP Architecture	396
8.6.3 NAP Access	397
8.7 Searching the Internet	399
8.7.1 Gathering Information: Spiders and Search Engines	399
8.7.2 Actual Search Tools	406
References	411

Chapter 9 Internet Resources: A Travelogue of Web Malls 415

9.1 Introduction	415
9.2 A Shopping Experience	415
9.3 A Travelogue	417
9.3.1 Search	419
9.3.2 The Shopper Super Site	420

9.3.3	The Shopper Super Site Search Screen	421
9.3.4	iMall	422
9.3.5	What You Find at iMall	423
9.3.6	Mall Directory	424
9.3.7	The Clothing Pavillion at iMall	425
9.3.8	Sterling Company	426
9.3.9	The Internet Mall	427
9.3.10	Amazon Books	428
9.3.11	The Internet Mall Search of the Mall	430
9.3.12	Shopping Malls	434
9.3.13	The Awesome "Mall of the Internet"	434

Part 4 Applications

Chapter 10	Advertising on the Internet: Issues and Technologies	447
10.1	Introduction	447
10.2	Advertising on the Web	447
10.2.1	Approach	451
10.2.2	Measuring Effectiveness	456
10.3	"Marketing 101"	456
10.3.1	Production Versus Marketing	457
10.3.2	Market, Products, and Customers	458
10.3.3	Marketing Research	458
10.3.4	Market Segmentation	459
10.3.5	Setting Prices	460
10.3.6	Product Distribution	460
10.3.7	Examples	461
10.4	Creating a Web Site	461
10.4.1	Setting up a Server	465
10.4.2	Designing Web Pages with an Eye to Advertisement	466
10.4.3	Connecting to the Internet	469
10.4.4	Maintaining a Web Server	469
10.5	Conclusion	469
	References	
Chapter 11	Electronic Publishing Issues, Approaches, Legalities, and Technologies	471
11.1	EP	473
11.1.1	Current Focus of EP	475
11.1.2	Economics of EP	478
11.1.3	EP Process	480
11.1.4	The EP Architecture	483
11.1.5	EP Tools	484
11.1.6	EP Retrieval and Dissemination	485
11.1.7	EP Pricing Methods/Billing	488
11.2	Web-Based EP	490
11.2.1	Baseline Issues	490
11.2.2	Application Tools	493
11.2.3	Publishing on the Internet	496
11.2.4	Electronic Journals on the Web	499
11.2.5	Comparative Analysis of EP Advantages and Disadvantages	500

11.3	Intellectual Property Issues in the Age of EP	503
11.3.1	Intellectual Property Rights	505
11.3.2	"Two Words" about Copyright Law	507
11.3.3	Examples of Cases Involving Copyright Infringement	512
11.3.4	"Two Words" about Trademark Law	513
11.3.5	EP Issues and Trademark Law	514
11.3.6	Example of Cases Involving Domain Name Infringement	515
11.3.7	"Two Words" about Patent Law	516
11.3.8	EP Issues and Patent Law	517
11.4	Intellectual Property Issues for Multimedia/Hypermedia Development	518
11.4.1	Threats	520
11.4.2	What Is Property?	521
11.4.3	More Thoughts of Laws Applicable to Information Repositories	523
11.4.4	Copyright and Inlining and Hyperlinking	532
11.4.5	International Issues	534
11.4.6	Piracy Protection	536
11.4.7	Fair Use	538
11.5	Conclusion	540
	References	541
	Appendix: An Example of Patent Analysis	544
Appendix A Table of Contents of SET Book II: Technical Specification		559
Appendix B Table of Contents of SET Book III: Formal Protocol Definition		561
Appendix C Recent Books Related to the Topic—Other Views		563
Index	615	