

Contents

Preface	xiii
1 Motivation for electronic payment	1
<i>References</i>	4
2 Characteristics of current payment systems	5
2.1 Cash payments	6
2.2 Payment through banks	7
2.2.1 <i>Payment by check</i>	7
2.2.2 <i>Payment by giro or credit transfer</i>	9
2.2.3 <i>Automated clearing house (ACH) payments</i>	9
2.2.4 <i>Wire transfer services</i>	11
2.3 Using payment cards	12
2.4 Consumer preferences in payment systems	14
2.5 Regulatory framework	15
<i>References</i>	17
3 Cryptographic techniques	19
3.1 Encryption and decryption	20
3.2 Symmetric encryption	21
3.2.1 <i>Data Encryption Standard (DES)</i>	22
3.2.2 <i>Triple DES</i>	26
3.2.3 <i>IDEA</i>	26
3.2.4 <i>Advanced Encryption Standard (AES)</i>	28
3.2.5 <i>RC2, RC4, and RC5</i>	30
3.3 Message digesting or hashing	33

3.3.1	<i>MD5</i>	34
3.3.2	<i>The Secure Hash Algorithm (SHA)</i>	34
3.4	Kerberos	35
3.4.1	<i>Overview of the Kerberos model</i>	35
3.4.2	<i>Obtaining a ticket</i>	37
3.4.3	<i>Service request</i>	38
3.5	Asymmetric or public-key encryption	38
3.5.1	<i>Properties of a public-key cryptosystem</i>	39
3.5.2	<i>Trapdoor one-way functions</i>	40
3.5.3	<i>Using public-key cryptosystems for authentication</i>	40
3.6	Digital signatures and enveloping	40
3.7	RSA	42
3.8	Elliptic curve cryptography	44
3.9	Public-key infrastructure (PKI)	45
3.9.1	<i>Certificates</i>	45
3.9.2	<i>Certification authorities</i>	46
3.9.3	<i>Attribute certificates</i>	47
3.10	Transport of security information	48
3.10.1	<i>Abstract syntax notation (ASN.1)</i>	49
3.10.2	<i>The X.509 directory authentication framework</i>	51
3.10.3	<i>PKCS cryptographic message syntax</i>	53
3.11	Dual signatures	54
3.12	Nonces	56
3.13	Blind signatures	57
3.14	Chip cards/smart cards	59
3.14.1	<i>Card types</i>	60
3.14.2	<i>Memory types and capacity</i>	61
3.14.3	<i>Physical specifications</i>	63
3.14.4	<i>Security</i>	63
3.14.5	<i>Public-key processing capabilities</i>	64
3.14.6	<i>Multiapplication cards</i>	65
3.14.7	<i>Java Card</i>	65
3.14.8	<i>MULTOS</i>	67
3.14.9	<i>Observers</i>	68
	<i>References</i>	69
4	Credit card-based systems	73
4.1	Mail order/telephone order (MOTO) transactions	76

4.2	Unsecured network payments	76
4.3	First Virtual	77
4.4	Once-off credit card numbers	80
4.5	The secure socket layer (SSL)	82
4.6	<i>i</i> -Key protocol (<i>i</i> KP)	89
4.6.1	<i>Framework of iKP protocols</i>	90
4.6.2	<i>1KP</i>	91
4.6.3	<i>2KP</i>	96
4.6.4	<i>3KP</i>	98
4.7	Secure Electronic Transactions (SET)	100
4.7.1	<i>The SET trust model</i>	102
4.7.2	<i>SET message structure</i>	105
4.7.3	<i>Payment initialization (PInitReq/PInitRes)</i>	106
4.7.4	<i>Purchase order (PReq/Pres)</i>	107
4.7.5	<i>Authorization (AuthReq/AuthRes)</i>	112
4.7.6	<i>Capture of payment (CapReq/CapRes)</i>	114
4.7.7	<i>Cardholder inquiry (InqReq/InqRes)</i>	115
4.7.8	<i>SET software components</i>	120
4.7.9	<i>SET market acceptance</i>	120
4.7.10	<i>Server-side wallets</i>	122
4.7.11	<i>Using SET with smart cards</i>	123
4.8	Summary	123
	<i>References</i>	125
5	Electronic checks and account transfers	127
5.1	Payment transfer between centralized accounts	128
5.1.1	<i>Funding the account</i>	130
5.1.2	<i>Authenticated account transfer</i>	134
5.1.3	<i>Withdrawing funds from the system</i>	137
5.1.4	<i>Business models</i>	137
5.2	FSTC payment initiatives	138
5.2.1	<i>Electronic check concept</i>	139
5.2.2	<i>Financial Services Markup Language (FSML)</i>	141
5.2.3	<i>Electronic check functional flows</i>	144
5.2.4	<i>Check-handling infrastructure</i>	146
5.2.5	<i>Bank Internet Payment System (BIPS)</i>	148
5.2.6	<i>Financial Agent Secure Transaction (FAST)</i>	151

5.3	NACHA Internet payments	153
5.3.1	<i>Internet Secure ATM Payments (ISAP)</i>	153
5.3.2	<i>DirectPay</i>	155
5.4	NetBill	156
5.4.1	<i>Protocol overview</i>	157
5.4.2	<i>Authentication procedure</i>	159
5.4.3	<i>Transaction protocol</i>	160
5.4.4	<i>Price request phase</i>	161
5.4.5	<i>Goods delivery phase</i>	161
5.4.6	<i>Payment phase</i>	162
5.4.7	<i>NetBill characteristics</i>	163
5.5	NetCheque	164
5.6	Summary	167
	<i>References</i>	167
6	Electronic cash payment systems	171
6.1	Ecash	172
6.1.1	<i>The Ecash model</i>	173
6.1.2	<i>Ecash coins</i>	174
6.1.3	<i>Coin keys</i>	174
6.1.4	<i>Double-spending prevention</i>	177
6.1.5	<i>Withdrawing coins</i>	178
6.1.6	<i>An Ecash purchase</i>	180
6.1.7	<i>Making the payment</i>	180
6.1.8	<i>Proving payment</i>	181
6.1.9	<i>Payment deposit</i>	182
6.1.10	<i>Integration with the Web</i>	182
6.1.11	<i>Ecash in the mail</i>	183
6.1.12	<i>Transferring Ecash</i>	183
6.1.13	<i>Lost coins</i>	184
6.1.14	<i>Ecash and crime</i>	184
6.1.15	<i>Magic Money</i>	186
6.1.16	<i>Remarks</i>	186
6.2	Project CAFE	186
6.2.1	<i>Goals of CAFE</i>	187
6.2.2	<i>Architecture</i>	188
6.2.3	<i>CAFE devices</i>	189

6.2.4	<i>Role of observers</i>	190
6.2.5	<i>Protocol overview</i>	190
6.2.6	<i>Off-line coins</i>	191
6.2.7	<i>The α protocol</i>	192
6.2.8	<i>The Γ protocol</i>	195
6.2.9	<i>Additional features</i>	196
6.2.10	<i>Remarks</i>	196
6.3	<i>NetCash</i>	196
6.3.1	<i>Framework/model</i>	197
6.3.2	<i>NetCash coins</i>	198
6.3.3	<i>Double-spending prevention</i>	199
6.3.4	<i>Coin transfer</i>	200
6.3.5	<i>Certificate of insurance</i>	200
6.3.6	<i>Basic purchase</i>	201
6.3.7	<i>Obtaining coins</i>	201
6.3.8	<i>Paying a merchant</i>	203
6.3.9	<i>Verifying coins</i>	204
6.3.10	<i>Providing limited anonymity</i>	204
6.3.11	<i>Merchant anonymity</i>	205
6.3.12	<i>Preventing anonymity</i>	206
6.3.13	<i>Clearing</i>	206
6.3.14	<i>Extensions</i>	207
6.3.15	<i>Preventing merchant fraud</i>	207
6.3.16	<i>Off-line protocols</i>	209
6.3.17	<i>Remarks</i>	210
6.4	<i>Mondex</i>	210
6.5	<i>EMV cash cards and CEPS</i>	213
6.5.1	<i>EMV2000</i>	214
6.5.2	<i>Common Electronic Purse Specification (CEPS)</i>	214
6.5.3	<i>Remarks</i>	220
6.6	<i>SmartAxis</i>	220
6.7	<i>Remarks</i>	222
	<i>References</i>	223
7	Micropayment systems	227
7.1	<i>Millicent</i>	228
7.1.1	<i>The Millicent model</i>	229

7.1.2	<i>Purchasing with Millicent</i>	231
7.1.3	<i>Scrip</i>	233
7.1.4	<i>Scrip structure</i>	234
7.1.5	<i>Scrip certificate generation</i>	235
7.1.6	<i>Scrip validation</i>	235
7.1.7	<i>Preventing double spending</i>	237
7.1.8	<i>Computation costs</i>	237
7.1.9	<i>Sending scrip over a network: the Millicent protocols</i>	237
7.1.10	<i>Scrip in the clear</i>	237
7.1.11	<i>Encrypted network connection</i>	237
7.1.12	<i>Request signatures</i>	241
7.1.13	<i>Performance</i>	243
7.1.14	<i>Millicent with the Web</i>	243
7.1.15	<i>Extensions</i>	244
7.1.16	<i>Summary</i>	245
7.2	SubScrip	245
7.2.1	<i>Basic SubScrip</i>	246
7.2.2	<i>Establishing a temporary account</i>	246
7.2.3	<i>Providing anonymity</i>	247
7.2.4	<i>A SubScrip ticket</i>	247
7.2.5	<i>A SubScrip purchase</i>	248
7.2.6	<i>Security and privacy</i>	248
7.2.7	<i>Protected SubScrip</i>	249
7.2.8	<i>Refunding SubScrip</i>	250
7.2.9	<i>Lost tickets</i>	250
7.3	PayWord	250
7.3.1	<i>PayWord user certificates</i>	251
7.3.2	<i>Revoked certificates</i>	253
7.3.3	<i>PayWord chains</i>	253
7.3.4	<i>Commitment to a PayWord chain</i>	254
7.3.5	<i>Spending PayWords</i>	255
7.3.6	<i>Variable-size payments</i>	256
7.3.7	<i>Redeeming spent PayWords</i>	257
7.3.8	<i>Computational costs</i>	257
7.3.9	<i>Extensions</i>	258
7.3.10	<i>Remarks</i>	258

7.4	iKP micropayment protocol	259
7.4.1	μ -3KP protocol	260
7.4.2	Repeated micropayments	261
7.4.3	Nonrepeated micropayments	264
7.4.4	Remarks	266
7.5	Hash chain trees	266
7.5.1	PayTree	268
7.5.2	Unbalanced One-way Binary Tree (UOBT)	270
7.6	MicroMint	273
7.6.1	The MicroMint model	274
7.6.2	MicroMint coins	274
7.6.3	Verifying a coin	275
7.6.4	Minting coins	276
7.6.5	Computational costs	277
7.6.6	Multiple coins per bin	278
7.6.7	Coin validity criterion	278
7.6.8	Preventing forgery	279
7.6.9	A MicroMint purchase	280
7.6.10	Double spending	280
7.6.11	Extensions	281
7.7	Probability-based micropayments	283
7.7.1	Bets using coin flips	284
7.7.2	Hash chain lottery tickets	286
7.8	Jalda	288
7.9	NewGenPay/IBM Micropayments	292
7.10	Banner advertising as a form of micropayment	296
7.11	Micropayments summary and analysis	297
	References	300
8	Mobile commerce	303
8.1	Mobile Internet architectures	305
8.1.1	Carrying Internet data on cellular networks	305
8.1.2	The wireless application protocol (WAP)	306
8.1.3	Japan's iMode service	307
8.2	Industry consortia	308
8.3	Mobile network operator as banker	308
8.4	Third-party account-based mobile payment systems	309
8.4.1	Sonera MobilePay	310

8.4.2	<i>Paybox</i>	311
8.4.3	<i>GiSMo</i>	313
8.4.4	<i>The Fundamo architecture</i>	315
8.5	Credit card-based systems	316
8.5.1	<i>Mobile SET</i>	317
8.5.2	<i>Remarks</i>	320
8.6	Summary	321
	<i>References</i>	322
9	Payment systems: prospects for the future	325
	About the authors	329
	Index	331