

# Contents

<b>Foreword</b>	<b>xv</b>
<b>Preface</b>	<b>xvii</b>
<b>About the Author</b>	<b>xxi</b>
<b>Chapter 1 The 3 “A”s: Authentication, Authorization, Accounting</b>	<b>1</b>
1.1 Authentication Concepts	1
1.1.1 Client Authentication	2
1.1.2 Message Authentication	4
1.1.3 Mutual Authentication	5
1.1.4 Models for Authentication Messaging	6
1.1.4.1 Two-Party Authentication Model	6
1.1.4.2 Three-Party Authentication Model	6
1.1.5 AAA Protocols for Authentication Messaging	7
1.1.5.1 User–AAA Server	7
1.1.5.2 NAS–AAA Server Communications	7
1.1.5.3 Supplicant (User)–NAS Communications	8
1.2 Authorization	8
1.2.1 How is it Different from Authentication?	8
1.2.2 Administration Domain and Relationships with the User	9
1.2.3 Standardization of Authorization Procedures	10
1.2.3.1 Authorization Messaging	12
1.2.3.2 Policy Framework and Authorization	12
1.3 Accounting	13
1.3.1 Accounting Management Architecture	13
1.3.1.1 Accounting Across Administrative Domains	14
1.3.2 Models for Collection of Accounting Data	15
1.3.2.1 Polling Models for Accounting	15
1.3.2.2 Event-Driven Models for Accounting	15
1.3.3 Accounting Security	17
1.3.4 Accounting Reliability	17
1.3.4.1 Interim Accounting	18
1.3.4.2 Transport Protocols	18
1.3.4.3 Fail-Over Mechanisms	18
1.3.5 Prepaid Service: Authorization and Accounting in Harmony	19
1.4 Generic AAA Architecture	19
1.4.1 Requirements on AAA Protocols Running on NAS	21

1.5 Conclusions and Further Resources	23
1.6 References	23
<b>Chapter 2 Authentication</b>	<b>25</b>
2.1 Examples of Authentication Mechanisms	25
2.1.1 User Authentication Mechanisms	26
2.1.1.1 Basic PPP User Authentication Mechanisms	27
2.1.1.2 Shortcoming of PPP Authentication Methods	29
2.1.1.3 Extensible Authentication Protocol (EAP) as Extension to PPP	30
2.1.1.4 SIM-Based Authentication	30
2.1.2 Example of Device Authentication Mechanisms	31
2.1.2.1 Public Key Certificate-Based Authentication	32
2.1.2.2 Basics of Certificate-Based Authentication	32
2.1.3 Examples of Message Authentication Mechanisms	33
2.1.3.1 HMAC-MD5	34
2.2 Classes of Authentication Mechanisms	36
2.2.1 Generic Authentication Mechanisms	41
2.2.1.1 Extensible Authentication Protocol (EAP)	41
2.2.1.2 EAP Messaging	42
2.3 Further Resources	44
2.4 References	45
<b>Chapter 3 Key Management Methods</b>	<b>47</b>
3.1 Key Management Taxonomy	47
3.1.1 Key Management Terminology	47
3.1.2 Types of Cryptographic Algorithms	49
3.1.3 Key Management Functions	50
3.1.4 Key Establishment Methods	51
3.1.4.1 Key Transport	51
3.1.4.2 Key Agreement	52
3.1.4.3 Manual Key Establishment	53
3.2 Management of Symmetric Keys	54
3.2.1 EAP Key Management Methods	54
3.2.2 Diffie–Hellman Key Agreement for Symmetric Key Generation	58
3.2.2.1 Problems with Diffie–Hellman	60
3.2.3 Internet Key Exchange for Symmetric Key Agreement	61
3.2.4 Kerberos and Single Sign On	62
3.2.4.1 Kerberos Issues	65
3.2.5 Kerberized Internet Negotiation of Keys (KINK)	66
3.3 Management of Public Keys and PKIs	67
3.4 Further Resources	68
3.5 References	69
<b>Chapter 4 Internet Security and Key Exchange Basics</b>	<b>71</b>
4.1 Introduction: Issues with Link Layer-Only Security	71
4.2 Internet Protocol Security	73
4.2.1 Authentication Header	74
4.2.2 Encapsulating Security Payload	74
4.2.3 IPsec Modes	75
4.2.3.1 Transport Mode	76
4.2.3.2 Tunnel Mode	76

Contents	ix
4.2.4 Security Associations and Policies	77
4.2.5 IPsec Databases	78
4.2.6 IPsec Processing	78
4.2.6.1 Outbound Processing	78
4.2.6.2 Inbound Processing	79
4.3 Internet Key Exchange for IPsec	79
4.3.1 IKE Specifications	79
4.3.2 IKE Conversations	81
4.3.2.1 IKE Phase 1	81
4.3.2.2 IKE Phase 2	82
4.3.2.3 Round Trip Optimizations	82
4.3.3 ISAKMP: The Backstage Protocol for IKE	83
4.3.3.1 ISAKMP Message Format	83
4.3.3.2 ISAKMP Payloads in IKE Conversations	86
4.3.4 The Gory Details of IKE	86
4.3.4.1 Derivation of ISAKMP Short-Term Keys	86
4.3.4.2 IKE Authentication Alternatives	88
4.3.4.3 IKE Deployment Issues	90
4.4 Transport Layer Security	91
4.4.1 TLS Handshake for Key Exchange	93
4.4.2 TLS Record Protocol	95
4.4.2.1 TLS Alert Protocol	95
4.4.3 Issues with TLS	96
4.4.4 Wireless Transport Layer Security	96
4.5 Further Resources	96
4.6 References	97
<b>Chapter 5 Introduction on Internet Mobility Protocols</b>	<b>99</b>
5.1 Mobile IP	99
5.1.1 Mobile IP Functional Overview	102
5.1.1.1 Mobile IP Registration	103
5.1.1.2 Mobile IP Reverse Tunneling	106
5.1.2 Mobile IP Messaging Security	107
5.1.2.1 Caveat: Key Establishment	109
5.2 Shortcomings of Mobile IP Base Specification	109
5.2.1 Mobile IP Bootstrapping Issues	110
5.2.1.1 Dynamic Home Address Assignment	111
5.2.1.2 Dynamic Home Agent Assignment	111
5.2.1.3 Dynamic Key Establishment	113
5.2.2 Mobile IP Handovers and Their Shortcomings	113
5.2.2.1 Layer-2 Triggers and Fast Handovers	114
5.2.2.2 Candidate Router Discovery Issues	115
5.2.2.3 Delay and Disruption Tolerance by Applications	116
5.2.2.4 Establishment of Network Services	116
5.3 Seamless Mobility Procedures	117
5.3.1 Candidate Access Router Discovery	118
5.3.2 Context Transfer	120
5.3.2.1 Design Considerations	122
5.3.2.2 Messaging Overview	124
5.4 Further Resources	125
5.5 References	126

<b>Chapter 6 Remote Access Dial-In User Service (RADIUS)</b>	<b>127</b>
6.1 RADIUS Basics	127
6.2 RADIUS Messaging	128
6.2.1 Message Format	129
6.2.2 RADIUS Extensibility	130
6.2.3 Transport Reliability for RADIUS	130
6.2.4 RADIUS and Security	131
6.2.4.1 RADIUS Message Integrity Protection	131
6.2.4.2 Attribute Hiding	132
6.2.4.3 Security Vulnerabilities of RADIUS	134
6.2.4.4 RADIUS over IPsec	135
6.3 RADIUS Operation Examples	135
6.3.1 RADIUS Support for PAP	135
6.3.2 RADIUS Support for CHAP	136
6.3.3 RADIUS Interaction with EAP	138
6.3.4 RADIUS Accounting	139
6.3.4.1 Basic Operation	139
6.3.4.2 Security and Reliability of RADIUS Accounting	140
6.4 RADIUS Support for Roaming and Mobility	141
6.4.1 RADIUS Support for Proxy Chaining	142
6.4.1.1 Roaming Concepts	142
6.4.1.2 Proxy Chaining Operation	143
6.4.1.3 Issues with Proxy Chaining	143
6.5 RADIUS Issues	143
6.6 Further Resources	144
6.6.1 Commercial RADIUS Resources	144
6.6.2 Free Open Source Material	145
6.7 References	145
<b>Chapter 7 Diameter: Twice the RADIUS?</b>	<b>147</b>
7.1 Election for the Next AAA Protocol	147
7.1.1 The Web of Diameter Specifications	148
7.1.1.1 Diameter Base Specification	148
7.1.1.2 Security Specifications	149
7.1.1.3 Diameter Transport Profile	150
7.1.1.4 Diameter NAS Application	150
7.1.2 Diameter Applications	151
7.1.3 Diameter Node Types and their Roles	152
7.2 Diameter Protocol	153
7.2.1 Diameter Messages	153
7.2.1.1 Diameter Message Format	154
7.2.1.2 Diameter Command Code (Message Types)	154
7.2.1.3 Attribute-Value Pair (AVP) Format	155
7.2.1.4 Examples of Diameter Base Specification AVPs	156
7.2.2 Diameter Transport and Routing Concepts	157
7.2.2.1 Diameter Transport Concepts	157
7.2.2.2 Diameter Routing Concepts	158
7.2.2.3 Diameter Message Routing and Forwarding	159
7.2.3 Capability Negotiations	159

7.2.4 Diameter Security Requirements	160
7.2.4.1 Use of IPsec or TLS for Diameter	161
7.2.4.2 Path Authorization: Impact of Security on Authorization and Accounting	161
7.3 Details of Diameter Applications	162
7.3.1 Accounting Message Exchange Example	162
7.3.2 Diameter-Based Authentication, NASREQ	163
7.3.2.1 Commands Introduced by NASREQ	164
7.3.2.2 NASREQ AVPs	164
7.3.2.3 Diameter NAS Messaging	165
7.3.3 Diameter Mobile IP Application	167
7.3.4 Diameter EAP Support	167
7.4 Diameter Versus RADIUS: A Factor 2?	168
7.4.1 Advantages of Diameter over RADIUS	168
7.4.1.1 Fail-Over	168
7.4.1.2 Server-initiated Messages	169
7.4.1.3 Reliable Transport	169
7.4.1.4 Capability Negotiation	169
7.4.1.5 Security and Audibility Issues	169
7.4.1.6 Diameter Support for Agents and Inter-Domain Roaming	170
7.4.1.7 Peer Discovery and Configuration	170
7.4.1.8 Backward Compatibility with RADIUS	170
7.4.2 Issues with Use of Diameter	170
7.4.3 Diameter-RADIUS Interactions (Translation Agents)	171
7.5 Further Resources	172
7.6 References	172
<b>Chapter 8 AAA and Security for Mobile IP</b>	<b>175</b>
8.1 Architecture and Trust Model	177
8.1.1 Timing Characteristics of Security Associations	178
8.1.1.1 Pre-established SAs (PSA)	178
8.1.1.2 Mobility Security Associations (MSA)	179
8.1.1.3 AAASA	179
8.1.1.4 Lifetimes	180
8.1.1.5 Security Parameter Index (SPI)	180
8.1.2 Key Delivery Mechanisms	181
8.1.3 Overview of Use of Mobile IP-AAA in Key Generation	182
8.2 Mobile IPv4 Extensions for Interaction with AAA	184
8.2.1 MN-AAA Authentication Extension	184
8.2.2 Key Generation Extensions (IETF work in progress)	186
8.2.3 Keys to Mobile IP Agents?	187
8.3 AAA Extensions for Interaction with Mobile IP	187
8.3.1 Diameter Mobile IPv4 Application	188
8.3.1.1 Diameter Model for Mobile IP Support	188
8.3.1.2 New Diameter AVPs for Mobile IP Support	190
8.3.1.3 Diameter Mobile IP Messaging Overview	193
8.3.2 Radius and Mobile IP Interaction: A CDMA2000 Example	196
8.3.2.1 Mobile IP Support Within CDMA2000	196
8.3.2.2 RADIUS Support, or Not!	197
8.3.2.3 CDMA2000 Messaging Procedure	199

8.4	Conclusion and Further Resources	200
8.5	References	201
<b>Chapter 9 PKI: Public Key Infrastructure: Fundamentals and Support for IPsec and Mobility</b>		<b>203</b>
9.1	Public Key Infrastructures: Concepts and Elements	204
9.1.1	Certificates	204
9.1.2	Certificate Management Concepts	205
9.1.3	PKI Elements	209
9.1.4	PKI Management Basic Functions	210
9.1.4.1	Basic PKI Transactions	211
9.1.4.2	Enrollment and Authentication	211
9.1.5	Comparison of Existing PKI Management Protocols	212
9.1.5.1	PKCS #10	213
9.1.5.2	SSL Protection for PKCS #10	214
9.1.5.3	PKCS #7 Protection for PKCS #10	215
9.1.5.4	IETF Certificate Management Protocol (CMP)	219
9.1.5.5	Certificate Management Using CMS (CMC)	221
9.1.5.6	Simple Certificate Enrollment Protocol (SCEP)	221
9.1.6	PKI Operation Protocols	221
9.1.6.1	PKI Certificate Discovery and Validation Protocols	222
9.2	PKI for Mobility Support	222
9.2.1	Identity Management for Mobile Clients: No IP Addresses!	222
9.2.1.1	Certificate Subjects for Mobile Devices	223
9.2.1.2	Certificate Subjects for Human Users	224
9.2.2	Certification and Distribution Issues	225
9.2.2.1	Validity Checking and CRL Distribution	225
9.2.2.2	Roaming and Certification	226
9.2.2.3	Device Certificates	226
9.2.2.4	User Certificates	226
9.3	Using Certificates in IKE	227
9.3.1	Exchange of Certificates within IKE	229
9.3.1.1	Certificate Data Type Profiling for ISAKMP	229
9.3.1.2	In-Band Versus Out-of-Band Exchanges	230
9.3.1.3	Certificate Authority and Certificate Chains	230
9.3.2	Identity Management for ISAKMP: No IP Address, Please!	231
9.4	Further Resources	232
9.5	References	232
9.6	Appendix A PKCS Documents	233
<b>Chapter 10 Latest Authentication Mechanisms, EAP Flavors</b>		<b>235</b>
10.1	Introduction	235
10.1.1	EAP Transport Mechanisms	237
10.1.2	EAP over LAN (EAPOL)	237
10.1.3	EAP over AAA Protocols	238
10.2	Protocol Overview	239
10.3	EAP-XXX	242
10.3.1	EAP-TLS (TLS over EAP)	244
10.3.1.1	EAP-TLS Architecture and Message Format	244
10.3.1.2	Protocol Overview	246
10.3.1.3	Drawbacks with EAP-TLS	248

Contents	<b>xiii</b>
10.3.2 EAP-TTLS	248
10.3.2.1 EAP-TTLS Functional Elements	250
10.3.2.2 Messaging Overview	252
10.3.2.3 Protocol Overview	253
10.3.2.4 Session Resumption: EAP-TTLS Support for Mobility	254
10.3.2.5 Example: CHAP Over EAP-TTLS	255
10.3.3 EAP-SIM	257
10.4 Use of EAP in 802 Networks	259
10.4.1 802.1X Port-Based Authentication	259
10.4.1.1 EAPOL in 802.1X and Interaction with RADIUS	260
10.4.1.2 Security Flaws of 802.1X, WPA/RSN and 802.1aa	260
10.4.2 Lightweight Extensible Authentication Protocol (LEAP)	260
10.4.3 PEAP	262
10.5 Further Resources	262
10.6 References	263
<b>Chapter 11 AAA and Identity Management for Mobile Access: The World of Operator Co-Existence</b>	<b>265</b>
11.1 Operator Co-existence and Agreements	265
11.1.1 Implications for the User	266
11.1.2 Implications for the Operators	267
11.1.3 Bilateral Billing and Trust Agreements and AAA Issues	269
11.1.3.1 Identity Management and Security Issues	271
11.1.4 Brokered Billing and Trust Agreements	272
11.1.5 Billing and Trust Management through an Alliance	274
11.2 A Practical Example: Liberty Alliance	275
11.2.1 Building the Trust Network: Identity Federation	276
11.2.1.1 Identity Services	276
11.2.1.2 Circle of Trust	278
11.2.1.3 Building the Circle of Trust	278
11.2.2 Support for Authentication/Sign On/Sign Off	279
11.2.2.1 Enabling Protocols	281
11.2.3 Advantages and Limitations of the Liberty Alliance	282
11.3 IETF Procedures	283
11.4 Further Resources	285
11.5 References	285
<b>Index</b>	<b>287</b>

