

Contents

Preface	ix
Acknowledgements	xi
1 Introduction	1
1.1 Authenticated Key Agreement	1
1.2 The Challenge in Authenticated Key Agreement	2
1.3 How to Read this Book?	5
Reference	6
2 Classical Approaches to Authentication and Key Agreement	7
2.1 Existing Mobile Security Solutions	7
2.1.1 UMTS Security Infrastructure	7
2.1.2 Issues in Securing Services with Radio Layer Security	14
2.2 General-Purpose Approaches to Authentication and Key Management	16
2.2.1 Public Key Infrastructure (PKI)	16
2.2.2 Passwords	18
2.2.3 Kerberos	19
2.2.4 Radio Layer and General Purpose Security Mechanisms	19
2.3 Requirements for GAA	20
References	21
3 Generic Authentication Architecture	23
3.1 Overview of Generic Authentication Architecture	23
3.1.1 Rationales for Design Decisions	23
3.1.2 A Bird's Eye View of GAA	25
3.2 Foundations of GAA	30
3.2.1 Architectural Elements of GAA	30
3.2.2 Bootstrapping	33
3.2.3 Authentication	39

3.3	Variations of the Generic Bootstrapping Architecture	41
3.3.1	<i>GBA_ME</i>	42
3.3.2	<i>GBA_U</i>	42
3.3.3	<i>2G GBA</i>	47
3.3.4	<i>Detection of Bootstrapping Variants by the NAF</i>	48
3.3.5	<i>3GPP2 GBA</i>	54
3.4	Building Blocks of GAA	66
3.4.1	<i>Introduction</i>	66
3.4.2	<i>PKI Portal</i>	72
3.4.3	<i>HTTPS Support</i>	74
3.4.4	<i>Key Distribution Service</i>	74
	3.4.4.1 Key Distribution for Terminal to Remote Device Usage	74
	3.4.4.2 Key Distribution for UICC to Terminal Usage	77
3.5	Other Architectural Issues	79
3.5.1	<i>Access Control Mechanisms in GAA</i>	79
	3.5.1.1 Local Policy Enforcement in the BSF	80
	3.5.1.2 USS usage for NAFs	81
3.5.2	<i>Identities in GAA</i>	82
3.5.3	<i>Identity Privacy and Unlinkability</i>	84
3.5.4	<i>Usability and GAA</i>	84
3.5.5	<i>Split Terminal</i>	87
3.5.6	<i>Interoperator GAA: Using GAA Across Operator Boundaries</i>	89
3.5.7	<i>Security Considerations of GAA</i>	91
3.6	Overview of 3GPP GAA Specifications	96
	References	100
4	Applications Using Generic Authentication Architecture	105
4.1	Standardized Usage Scenarios	105
4.1.1	<i>Authentication Using GAA</i>	105
	4.1.1.1 HTTP Digest Authentication	107
	4.1.1.2 Pre-Shared Key TLS	111
	4.1.1.3 Proxy Mode Authentication	112
	4.1.1.4 Referrer Mode Authentication	116
4.1.2	<i>Broadcast Mobile TV Service</i>	119
	4.1.2.1 Security Goals	123
	4.1.2.2 Service Architecture	123
	4.1.2.3 Message Flow Example	126
	4.1.2.4 Tracing Source of Leaked Keys	130
4.1.3	<i>Further Standardized Usage Scenarios</i>	131
4.2	Additional Usage Scenarios	135
4.2.1	<i>Secure Enterprise Login</i>	136
4.2.2	<i>Personalization for Payments and Securing Public Transport Tickets</i>	138
4.2.3	<i>Secure Messaging in Delay and Disruption-prone Environments</i>	140
4.2.4	<i>Terminal to Terminal Security</i>	141

4.2.5 <i>Transitive Trust in IP Multimedia Subsystems (IMS)</i>	144
References	148
5 Guidance for Deploying GAA	153
5.1 Integration with Application Servers	153
5.1.1 <i>Introduction</i>	153
5.1.2 <i>Username / Password Replacement</i>	154
5.1.3 <i>NAF Library</i>	155
5.1.3.1 <i>Apache Web Server</i>	156
5.1.3.2 <i>J2EE Servers</i>	157
5.1.3.3 <i>Direct Usage of NAF Library</i>	158
5.1.4 <i>Web Services Direct Usage</i>	159
5.2 Integration with OS Security	159
5.2.1 <i>Threats for GAA Implementations in Open Platform UEs</i>	160
5.2.2 <i>Access Control Requirements</i>	161
5.2.3 <i>Basic Access Control in Practice: Integration in the Series 60 Platform</i>	162
5.2.4 <i>Extended Access Control: Design Options</i>	163
5.2.5 <i>Other Platforms</i>	165
5.3 Integration with Identity Management Systems	166
5.3.1 <i>Introduction</i>	166
5.3.2 <i>GAA Interworking with Liberty ID-FF</i>	167
5.4 Integration of GAA into Mobile Networks	170
5.4.1 <i>Integration of HLR into GAA</i>	170
5.4.2 <i>Key Lifetime Setting in BSF</i>	173
5.4.3 <i>Usage of SIM Cards in GAA (2G GBA)</i>	175
5.4.4 <i>Charging and GAA</i>	177
5.4.5 <i>GAA Integration into Large Networks</i>	178
References	180
6 Future Trends	183
6.1 Standardization Outlook	183
6.1.1 <i>GBA Push</i>	183
6.1.2 <i>GAA User Privacy</i>	185
6.1.3 <i>GAA in Evolved Packet Systems (EPSs) and Mobile IP (MIP)</i>	187
6.2 Outlook for GAA	189
References	192
Terminology and Abbreviations	193
Index	201

