

1. Record Nr.	UNINA9910830674803321
Autore	Forsberg Dan
Titolo	LTE security // Dan Forsberg ... [et al.]
Pubbl/distr/stampa	Chichester, West Sussex ; , : John Wiley & Sons, , 2013 [Piscataway, New Jersey] : , : IEEE Xplore, , [2012]
ISBN	1-118-38064-9 1-299-18726-9 1-118-38067-3 1-118-38065-7
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (367 p.)
Collana	Nsn/nokia series
Altri autori (Persone)	HornGunther MoellerWolf-Dietrich NiemiValtteri
Disciplina	621.3845/6 621.38456
Soggetti	Long-Term Evolution (Telecommunications) Global system for mobile communications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	-- Preface xiii -- Foreword to the First Edition xv -- Acknowledgements xix -- Copyright Acknowledgements xix -- 1 Overview of the Book 1 -- 2 Background 5 -- 2.1 Evolution of Cellular Systems 5 -- 2.2 Basic Security Concepts 10 -- 2.3 Basic Cryptographic Concepts 13 -- 2.4 Introduction to LTE Standardization 21 -- 2.5 Notes on Terminology and Specification Language 26 -- 3 GSM Security 29 -- 3.1 Principles of GSM Security 29 -- 3.2 The Role of the SIM 30 -- 3.3 Mechanisms of GSM Security 31 -- 3.4 GSM Cryptographic Algorithms 34 -- 4 Third-Generation Security (UMTS) 37 -- 4.1 Principles of Third-Generation (3G) Security 37 -- 4.2 Third-Generation Security Mechanisms 40 -- 4.3 Third-Generation Cryptographic Algorithms 49 -- 4.4 Interworking between GSM and 3G Security 55 -- 4.5 Network Domain Security 59 -- 4.6 Architectures with RNCs in Exposed Locations 65 -- 5 3G / WLAN Interworking 67 -- 5.1 Principles of 3G / WLAN Interworking 67 -- 5.2 Security Mechanisms of

3G / WLAN Interworking	75
5.3 Cryptographic Algorithms for 3G / WLAN Interworking	81
6 EPS Security Architecture	83
6.1 Overview and Relevant Specifications	83
6.2 Requirements and Features of EPS Security	89
6.3 Design Decisions for EPS Security	97
6.4 Platform Security for Base Stations	103
7 EPS Authentication and Key Agreement	109
7.1 Identification	109
7.2 The EPS Authentication and Key Agreement Procedure	112
7.3 Key Hierarchy	123
7.4 Security Contexts	129
8 EPS Protection for Signalling and User Data	133
8.1 Security Algorithms Negotiation	133
8.2 NAS Signalling Protection	136
8.3 AS Signalling and User Data Protection	138
8.4 Security on Network Interfaces	141
8.5 Certificate Enrollment for Base Stations	143
8.6 Emergency Call Handling	151
9 Security in Intra-LTE State Transitions and Mobility	155
9.1 Transitions to and from Registered State	156
9.2 Transitions between Idle and Connected States	157
9.3 Idle State Mobility	158
9.4 Handover	161
9.5 Key Change on the Fly	169
9.6 Periodic Local Authentication Procedure	170
9.7 Concurrent Run of Security Procedures	171
10 EPS Cryptographic Algorithms	175
10.1 Null Algorithms	176
10.2 Ciphering Algorithms	177
10.3 Integrity Algorithms	180
10.4 Key Derivation Algorithms	180
11 Interworking Security between EPS and Other Systems	183
11.1 Interworking with GSM and 3G Networks	183
11.2 Interworking with Non-3GPP Networks	193
12 Security for Voice over LTE	215
12.1 Methods for Providing Voice over LTE	215
12.2 Security Mechanisms for Voice over LTE	220
12.3 Rich Communication Suite and Voice over LTE	230
13 Security for Home Base Station Deployment	233
13.1 Security Architecture, Threats and Requirements	234
13.2 Security Features	241
13.3 Security Procedures Internal to the Home Base Station	244
13.4 Security Procedures between Home Base Station and Security Gateway	247
13.5 Security Aspects of Home Base Station Management	261
13.6 Closed Subscriber Groups and Emergency Call Handling	275
13.7 Support for Subscriber Mobility	277
14 Relay Node Security	281
14.1 Overview of Relay Node Architecture	281
14.2 Security Solution	284
15 Security for Machine-Type Communications	293
15.1 Security for MTC at the Application Level	294
15.2 Security for MTC at the 3GPP Network Level	301
15.3 Security for MTC at the Credential Management Level	306
16 Future Challenges	309
16.1 Near-Term Outlook	309
16.2 Far-Term Outlook	314
Abbreviations	319
References	327
Index	337

Sommario/riassunto

A concise, updated guide to LTE Security This is a welcome Second Edition of the successful book on LTE Security (2010) addressing the security architecture for LTE as specified by 3GPP. Since 2010, LTE has established itself as the unrivalled mobile broadband technology of the fourth generation (4G), with significant commercial deployments around the world and a fast growing market. The subject of this book is hence even more relevant than it has been at the time of the first edition. The authors explain in detail the security mechanisms employed in LTE and give an overview of the ones in GSM and 3G, which LTE security substantially extends. The specifications generated by standardization bodies inform how to implement the system (and this only to the extent required for interoperability), but almost never inform readers about why things are done the way they are. Furthermore, specifications tend to be readable only for a small group of experts and lack the context of the broader picture. LTE Security Second Edition describes the essential elements of LTE Security, written by leading experts who participated in decisively shaping LTE security in the relevant standardization body, 3GPP, and explains the rationale

behind the standards specifications giving readers a broader understanding of the context to these specifications. . Includes two new chapters covering 3GPP work on Relay Node Security and on system enhancements for Machine-type Communication (MTC), plus application layer security in ETSI TC M2M and embedded smart card in ETSI SCP . Updates existing chapters , including Voice over LTE, Home base stations, and New Cryptographic Algorithms.
