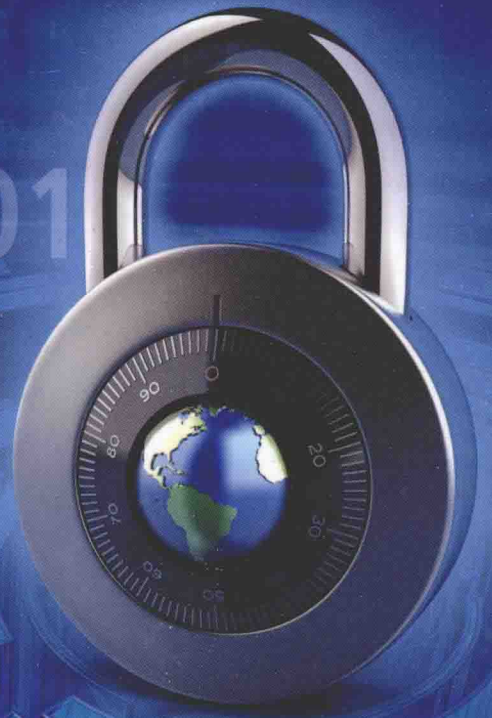


Second Edition

LTE Security

Dan Forsberg | Günther Horn
Wolf-Dietrich Moeller | Valtteri Niemi



LTE SECURITY

Second Edition

Dan Forsberg

Poplatek Oy, Finland

Günther Horn

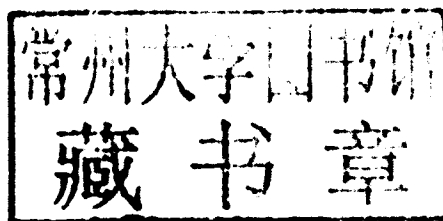
Nokia Siemens Networks, Germany

Wolf-Dietrich Moeller

Nokia Siemens Networks, Germany

Valtteri Niemi

University of Turku and Nokia Corporation, Finland



 **WILEY**

A John Wiley & Sons, Ltd., Publication

This edition first published 2013
© 2013 John Wiley and Sons Ltd

Registered office

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

LTE security / Gunther Horn ... [et al.]. – 2nd ed.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-118-35558-9 (cloth)

1. Long-Term Evolution (Telecommunications) 2. Global system for mobile communications.
I. Horn, Gunther.

TK5103.48325.L74 2013

621.3845'6–dc23

2012025771

A catalogue record for this book is available from the British Library.

ISBN: 9781118355589

Set in 10/12pt Times by Laserwords Private Limited, Chennai, India

Printed and bound in Singapore by Markono Print Media Pte Ltd

LTE SECURITY

Preface

This is the second edition of the book *LTE Security* whose first edition appeared in the autumn of 2010.

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 was at the time of the first edition.

The basic specifications for LTE in general, and LTE security in particular, have proven remarkably stable since their first versions were published in 2008 as part of 3GPP Release 8. Nevertheless, as is quite common in the standardization process, a number of corrections to the LTE security specifications have been agreed since to fix shortcomings that had become apparent during the development and deployment processes.

More importantly, new features have been added to LTE to enhance support for new types of deployment scenarios and applications. From a security point of view, the most important of these additions are the support for relay nodes and for machine-type communications. We therefore devote two new chapters to them.

A number of other new features have been added to LTE security since 2010, one example being the addition of a third family of cryptographic algorithms for LTE. These new features have been added to the chapters that had existed already in the first edition of the book.

This book focuses on LTE security, but also gives a thorough introduction to its predecessors, GSM security and 3G security. The second edition updates the reader on recent developments in these areas. While things were quite calm on the 3G security front, confidence in the strength of some cryptographic algorithms used with GSM has been further eroded by live hacking demonstrations at a number of public events. These developments suggest that it is now time to take those stronger GSM algorithms into use that have already been standardized and are available in products.

Some of the topics mentioned in the last chapter of the first edition that provided an outlook have matured in the meantime and been included in the other chapters of the book. The outlook has been updated accordingly.

Summing up, this second edition includes the following updates with respect to the first edition:

- Two new chapters, on relay nodes and machine-type communications, have been added.

- All enhancements to LTE security specified for 3GPP Releases 10 and 11 have been included.
- All corrections to the specifications up to and including Release 11 and approved by 3GPP by June 2012 have been taken into account as far as they affect the text in the book.
- Major developments since 2010 affecting GSM security and 3G security are explained.
- The last chapter of the book providing an outlook to future developments has been updated.

Foreword to the First Edition

The early to mid-1980s saw the commercial opening across Europe of public-access mobile communications systems. These cellular systems all used analogue technology, but outside of the Nordic countries no attempt was made to standardize the systems – so the technology adopted differed from country to country. Unfortunately, one thing they did have in common was a total absence of adequate security features, which made them open to abuse by criminals, journalists and all manner of opportunists. Users' calls could be eavesdropped on the air using readily available and comparatively inexpensive interception devices, and there were celebrated cases of journalistic invasion of privacy. A well-known example was the 'squidgy' tapes, where mobile telephone calls between members of the British royal family were recorded. Mobile telephone operators and their customers became very concerned.

The operators also had another problem with serious financial consequences. When a mobile phone attempted to connect to a network, the only check made on authenticity was to see that the telephone number and the phone's identity correctly corresponded. These numbers could be intercepted on the air and programmed to new phones creating clones of the original. Clones were used by criminals to run up huge charges for calls which had nothing to do with the legitimate owner. Cloning became very widespread, with criminals placing their 'cloning' equipment in cars parked at airports to capture the numbers from business people announcing their arrival back home to their families. It represented a serious financial problem for operators who ended up covering the charges themselves. The problems caused by lack of security in European analogue systems were a significant factor in accelerating the creation and adoption of GSM.

GSM is a standard for digital mobile communications, designed originally for Europe but now adopted all over the world. Being an international standard it brings economy of scale and competition, and it enables users to roam across borders from one network to another. Being digital it brings transmission efficiency and flexibility, and enables the use of advanced cryptographic security. The security problems of the original analogue systems are addressed in GSM by encryption on the air interface of user traffic, in particular voice calls, and authentication by network operators of their customers on an individual basis whenever they attempt to connect to a network, irrespective of where that network may be. From both a technical and a regulatory perspective, the use of cryptography in GSM was groundbreaking. Initially manufacturers and operators feared it would add too much complexity to the system, and security agencies were concerned

that it may be abused by criminals and terror organizations. The legitimate fears and concerns constrained what was possible, especially with the encryption algorithm, which was designed against a philosophy of ‘minimum strength to provide adequate security’. Despite this, and the continuing efforts of organized hackers, eavesdropping on the air of GSM calls protected using the original cipher has still to be demonstrated in a real deployment, and with a stronger cipher already available in the wings, any future success will be largely pointless. This doesn’t mean that GSM is free from security weaknesses – the ability to attack it using false base stations is very real.

GSM is the first in an evolving family of technologies for mobile communications. The second member of the family is 3G (or UMTS, as it is often referred to in Europe) and the third, and most recent, is LTE EPS to give it its proper title which is used throughout the main body of this book). With each technology evolution the security features have been enhanced to address learning from its predecessor, as well as to accommodate any changes in system architecture or services. The underlying GSM security architecture has proved to be extremely robust, and consequently has remained largely unchanged with the evolving technology family. It has also been adapted for use in other communications systems, including WLAN, IMS and HTTP. It is characterized by authentication data and encryption key generation being confined to a user’s home network authentication centre and personal SIM, the two elements where all user-specific static security data is held. Only dynamic and user session-specific security data goes outside these domains.

3G sees the addition to the GSM security features of user authentication of the access network – to complement user authentication by the network, integrity protection of signalling and the prevention of authentication replay. Start and termination of ciphering are moved from the base station further into the network. Of course, the false base station attack is countered. A new suite of cryptographic algorithms based on algorithms open to public scrutiny and analysis is introduced, and changes of regulation governing the export of equipment with cryptographic functionality make their adoption easier for most parts of the world.

LTE heralds the first technology in the family that is entirely packet-switched – so voice security has to be addressed in an entirely different way from GSM and 3G. LTE is a much flatter architecture, with fewer network elements, and is entirely IP-based. Functionality, including security functionality, is migrated to the edge of the network, including encryption functionality which is moved to the edge of the radio network, having been moved from the base station to the radio network controller in the evolution from GSM to 3G. While maintaining compatibility with the security architecture developed for GSM and evolved for 3G, the security functionality has been significantly adapted, enhanced and extended to accommodate the changes that LTE represents, as well as security enhancements motivated by practical experience with 3G. Much of this plays back into 3G itself as new security challenges arise with the advent of femto cells – low-cost end nodes in exposed environments that are not necessarily under the control of the operator of the network to which they are attached.

The book takes the reader through the evolution of security across three generations of mobile, focussing with clarity and rigour on the security of LTE. It is co-authored by a team who continue to be at the heart of the working group in 3GPP responsible for defining the LTE security standards. Their knowledge, expertise and enthusiasm for the subject shine through.

Professor Michael Walker
Chairman of the ETSI Board

Acknowledgements

This book presents the results of research and specification work by many people over an extended period. Our thanks therefore go to all those who helped make Long Term Evolution (LTE) possible through their hard work. In particular, we thank the people working in 3GPP, the standardization body that publishes the LTE specifications, and, especially, the delegates to the 3GPP security working group, SA3, with whom we were working to produce the LTE security specifications over the past years.

We would also like to express our gratitude to our colleagues at Nokia and Nokia Siemens Networks for our longstanding fruitful collaboration. We are particularly indebted to N. Asokan, Wolfgang Bücker, Devaki Chandramouli, Jan-Erik Ekberg, Christian Günther, Silke Holtmanns, Jan Käll, Raimund Kausl, Rainer Liebhart, Christian Markwart, Kaisa Nyberg, Martin Öttl, Jukka Ranta, Manfred Schäfer, Peter Schneider, Hanns-Jürgen Schwarzbauer, José Manuel Tapia Pérez, Janne Tervonen, Robert Zaus and Dajiang Zhang who helped us improve the book through their invaluable comments.

Finally, we would like to thank the editing team at Wiley whose great work turned our manuscript into a coherent book.

The authors welcome any comments or suggestions for improvements.

Copyright Acknowledgements

The authors would like to include additional thanks and full copyright acknowledgement as requested by the following copyright holders in this book.

- © **2009, 3GPP™**. TSs and TRs are the property of ARIB, ATIS CCSA, ETSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided here ‘as is’ for information purposes only. Further use is strictly prohibited.
- © **2010, 3GPP™**. TSs and TRs are the property of ARIB, ATIS CCSA, ETSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided here ‘as is’ for information purposes only. Further use is strictly prohibited.
- © **2010, Nokia Corporation**. For permission to reproduce the Nokia Corporation UE icon within Figures 2.1, 3.1, 3.2, 3.3, 6.1, 6.2, 6.3, 7.1 and 14.1.
- © **2011, European Telecommunications Standards Institute**. Further use, modification, copy and/or distribution are strictly prohibited. ETSI standards are available from <http://pda.etsi.org/pda/>.

- © 2012, 3GPP™. TSs and TRs are the property of ARIB, ATIS CCSA, ETSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided here ‘as is’ for information purposes only. Further use is strictly prohibited.
- © 2012, GSM Association GSM™ and its licensors. All Rights Reserved.

Please see the individual figure and table captions and the footnotes to extracts from 3GPP specifications for copyright notices throughout the book.

Contents

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
2.1.1 <i>Third-Generation Network Architecture</i>	6
2.1.2 <i>Important Elements of the 3G Architecture</i>	7
2.1.3 <i>Functions and Protocols in the 3GPP System</i>	8
2.1.4 <i>The EPS System</i>	9
2.2 Basic Security Concepts	10
2.2.1 <i>Information Security</i>	10
2.2.2 <i>Design Principles</i>	11
2.2.3 <i>Communication Security Features</i>	12
2.3 Basic Cryptographic Concepts	13
2.3.1 <i>Cryptographic Functions</i>	14
2.3.2 <i>Securing Systems with Cryptographic Methods</i>	16
2.3.3 <i>Symmetric Encryption Methods</i>	17
2.3.4 <i>Hash Functions</i>	18
2.3.5 <i>Public-Key Cryptography and PKI</i>	19
2.3.6 <i>Cryptanalysis</i>	20
2.4 Introduction to LTE Standardization	21
2.4.1 <i>Working Procedures in 3GPP</i>	22
2.5 Notes on Terminology and Specification Language	26
2.5.1 <i>Terminology</i>	26
2.5.2 <i>Specification Language</i>	27
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
3.3.1	<i>Subscriber Authentication in GSM</i>	32
3.3.2	<i>GSM Encryption</i>	32
3.3.3	<i>GPRS Encryption</i>	33
3.3.4	<i>Subscriber Identity Confidentiality</i>	34
3.4	GSM Cryptographic Algorithms	34
4	Third-Generation Security (UMTS)	37
4.1	Principles of Third-Generation (3G) Security	37
4.1.1	<i>Elements of GSM Security Carried over to 3G</i>	37
4.1.2	<i>Weaknesses in GSM Security</i>	38
4.1.3	<i>Higher Level Objectives</i>	39
4.2	Third-Generation Security Mechanisms	40
4.2.1	<i>Authentication and Key Agreement</i>	40
4.2.2	<i>Ciphering Mechanism</i>	45
4.2.3	<i>Integrity Protection Mechanism</i>	46
4.2.4	<i>Identity Confidentiality Mechanism</i>	48
4.3	Third-Generation Cryptographic Algorithms	49
4.3.1	<i>KASUMI</i>	50
4.3.2	<i>UEA1 and UIA1</i>	51
4.3.3	<i>SNOW3G, UEA2 and UIA2</i>	51
4.3.4	<i>MILENAGE</i>	54
4.3.5	<i>Hash Functions</i>	54
4.4	Interworking between GSM and 3G Security	55
4.4.1	<i>Interworking Scenarios</i>	55
4.4.2	<i>Cases with SIM</i>	56
4.4.3	<i>Cases with USIM</i>	57
4.4.4	<i>Handovers between GSM and 3G</i>	58
4.5	Network Domain Security	59
4.5.1	<i>Generic Security Domain Framework</i>	59
4.5.2	<i>Security Mechanisms for NDS</i>	62
4.5.3	<i>Application of NDS</i>	64
4.6	Architectures with RNCs in Exposed Locations	65
5	3G–WLAN Interworking	67
5.1	Principles of 3G–WLAN Interworking	67
5.1.1	<i>The General Idea</i>	67
5.1.2	<i>The EAP Framework</i>	69
5.1.3	<i>Overview of EAP-AKA</i>	72
5.2	Security Mechanisms of 3G–WLAN Interworking	75
5.2.1	<i>Reference Model for 3G–WLAN Interworking</i>	75
5.2.2	<i>Security Mechanisms of WLAN Direct IP Access</i>	76
5.2.3	<i>Security Mechanisms of WLAN 3GPP IP Access</i>	78
5.3	Cryptographic Algorithms for 3G–WLAN Interworking	81

6	EPS Security Architecture	83
6.1	Overview and Relevant Specifications	83
6.1.1	<i>Need for Security Standardization</i>	85
6.1.2	<i>Relevant Nonsecurity Specifications</i>	87
6.1.3	<i>Security Specifications for EPS</i>	88
6.2	Requirements and Features of EPS Security	89
6.2.1	<i>Threats against EPS</i>	90
6.2.2	<i>EPS Security Features</i>	91
6.2.3	<i>How the Features Meet the Requirements</i>	95
6.3	Design Decisions for EPS Security	97
6.4	Platform Security for Base Stations	103
6.4.1	<i>General Security Considerations</i>	103
6.4.2	<i>Specification of Platform Security</i>	103
6.4.3	<i>Exposed Position and Threats</i>	103
6.4.4	<i>Security Requirements</i>	104
7	EPS Authentication and Key Agreement	109
7.1	Identification	109
7.1.1	<i>User Identity Confidentiality</i>	110
7.1.2	<i>Terminal Identity Confidentiality</i>	111
7.2	The EPS Authentication and Key Agreement Procedure	112
7.2.1	<i>Goals and Prerequisites of EPS AKA</i>	112
7.2.2	<i>Distribution of EPS Authentication Vectors from HSS to MME</i>	114
7.2.3	<i>Mutual Authentication and Establishment of a Shared Key between the Serving Network and the UE</i>	118
7.2.4	<i>Distribution of Authentication Data inside and between Serving Networks</i>	122
7.3	Key Hierarchy	123
7.3.1	<i>Key Derivations</i>	124
7.3.2	<i>Purpose of the Keys in the Hierarchy</i>	125
7.3.3	<i>Cryptographic Key Separation</i>	127
7.3.4	<i>Key Renewal</i>	128
7.4	Security Contexts	129
7.4.1	<i>EPS Security Context</i>	129
7.4.2	<i>EPS NAS Security Context</i>	130
7.4.3	<i>UE Security Capabilities</i>	130
7.4.4	<i>EPS AS Security Context</i>	130
7.4.5	<i>Native versus Mapped Contexts</i>	130
7.4.6	<i>Current versus Non-current Contexts</i>	131
7.4.7	<i>Key Identification</i>	131
7.4.8	<i>EPS Security Context Storage</i>	131
7.4.9	<i>EPS Security Context Transfer</i>	132
8	EPS Protection for Signalling and User Data	133
8.1	Security Algorithms Negotiation	133
8.1.1	<i>Mobility Management Entities</i>	134

8.1.2	<i>Base Stations</i>	135
8.2	NAS Signalling Protection	136
8.2.1	<i>NAS Security Mode Command Procedure</i>	136
8.2.2	<i>NAS Signalling Protection</i>	137
8.3	AS Signalling and User Data Protection	138
8.3.1	<i>AS Security Mode Command Procedure</i>	138
8.3.2	<i>RRC Signalling and User Plane Protection</i>	138
8.3.3	<i>RRC Connection Re-establishment</i>	140
8.4	Security on Network Interfaces	141
8.4.1	<i>Application of NDS to EPS</i>	141
8.4.2	<i>Security for Network Interfaces of Base Stations</i>	142
8.5	Certificate Enrolment for Base Stations	143
8.5.1	<i>Enrolment Scenario</i>	143
8.5.2	<i>Enrolment Principles</i>	144
8.5.3	<i>Enrolment Architecture</i>	147
8.5.4	<i>CMPv2 Protocol and Certificate Profiles</i>	148
8.5.5	<i>CMPv2 Transport</i>	149
8.5.6	<i>Example Enrolment Procedure</i>	150
8.6	Emergency Call Handling	151
8.6.1	<i>Emergency Calls with NAS and AS Security Contexts in Place</i>	153
8.6.2	<i>Emergency Calls without NAS and AS Security Contexts</i>	153
8.6.3	<i>Continuation of the Emergency Call When Authentication Fails</i>	154
9	Security in Intra-LTE State Transitions and Mobility	155
9.1	Transitions to and from Registered State	156
9.1.1	<i>Registration</i>	156
9.1.2	<i>Deregistration</i>	156
9.2	Transitions between Idle and Connected States	157
9.2.1	<i>Connection Initiation</i>	158
9.2.2	<i>Back to Idle State</i>	158
9.3	Idle State Mobility	158
9.4	Handover	161
9.4.1	<i>Handover Key Management Requirements Background</i>	161
9.4.2	<i>Handover Keying Mechanisms Background</i>	162
9.4.3	<i>LTE Key Handling in Handover</i>	166
9.4.4	<i>Multiple Target Cell Preparations</i>	168
9.5	Key Change on the Fly	169
9.5.1	<i>K_{eNB} Rekeying</i>	169
9.5.2	<i>K_{eNB} Refresh</i>	169
9.5.3	<i>NAS Key Rekeying</i>	170
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
11.1.1	<i>Routing Area Update Procedure in UTRAN or GERAN</i>	186
11.1.2	<i>Tracking Area Update Procedure in EPS</i>	187
11.1.3	<i>Handover from EPS to 3G or GSM</i>	190
11.1.4	<i>Handover from 3G or GSM to EPS</i>	191
11.2	Interworking with Non-3GPP Networks	193
11.2.1	<i>Principles of Interworking with Non-3GPP Networks</i>	193
11.2.2	<i>Authentication and Key Agreement for Trusted Access</i>	201
11.2.3	<i>Authentication and Key Agreement for Untrusted Access</i>	205
11.2.4	<i>Security for Mobile IP Signalling</i>	208
11.2.5	<i>Mobility between 3GPP and Non-3GPP Access Networks</i>	211
12	Security for Voice over LTE	215
12.1	Methods for Providing Voice over LTE	215
12.1.1	<i>IMS over LTE</i>	216
12.1.2	<i>Circuit Switched Fallback (CSFB)</i>	218
12.1.3	<i>Single Radio Voice Call Continuity (SRVCC)</i>	218
12.2	Security Mechanisms for Voice over LTE	220
12.2.1	<i>Security for IMS over LTE</i>	220
12.2.2	<i>Security for Circuit Switched Fallback</i>	228
12.2.3	<i>Security for Single Radio Voice Call Continuity</i>	228
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
13.1.1	<i>Scenario</i>	234
13.1.2	<i>Threats and Risks</i>	237
13.1.3	<i>Requirements</i>	239
13.1.4	<i>Security Architecture</i>	240
13.2	Security Features	241
13.2.1	<i>Authentication</i>	241
13.2.2	<i>Local Security</i>	243
13.2.3	<i>Communications Security</i>	244
13.2.4	<i>Location Verification and Time Synchronization</i>	244
13.3	Security Procedures Internal to the Home Base Station	244
13.3.1	<i>Secure Boot and Device Integrity Check</i>	245
13.3.2	<i>Removal of Hosting Party Module</i>	245
13.3.3	<i>Loss of Backhaul Link</i>	245
13.3.4	<i>Secure Time Base</i>	246
13.3.5	<i>Handling of Internal Transient Data</i>	246
13.4	Security Procedures between Home Base Station and Security Gateway	247
13.4.1	<i>Device Integrity Validation</i>	247

13.4.2	<i>Device Authentication</i>	247
13.4.3	<i>IKEv2 and Certificate Profiling</i>	250
13.4.4	<i>Certificate Processing</i>	253
13.4.5	<i>Combined Device-Hosting Party Authentication</i>	255
13.4.6	<i>Authorization and Access Control</i>	256
13.4.7	<i>IPsec Tunnel Establishment</i>	258
13.4.8	<i>Verification of HeNB Identity and CSG Access</i>	258
13.4.9	<i>Time Synchronization</i>	260
13.5	Security Aspects of Home Base Station Management	261
13.5.1	<i>Management Architecture</i>	261
13.5.2	<i>Management and Provisioning during Manufacturing</i>	264
13.5.3	<i>Preparation for Operator-Specific Deployment</i>	266
13.5.4	<i>Relationships between HeNB Manufacturer and Operator</i>	267
13.5.5	<i>Security Management in Operator Network</i>	267
13.5.6	<i>Protection of Management Traffic</i>	268
13.5.7	<i>Software Download</i>	270
13.5.8	<i>Location Verification</i>	272
13.6	Closed Subscriber Groups and Emergency Call Handling	275
13.6.1	<i>UE Access Control to HeNBs</i>	275
13.6.2	<i>Emergency Calls</i>	276
13.7	Support for Subscriber Mobility	277
13.7.1	<i>Mobility Scenarios</i>	277
13.7.2	<i>Direct Interfaces between HeNBs</i>	278
14	Relay Node Security	281
14.1	Overview of Relay Node Architecture	281
14.1.1	<i>Basic Relay Node Architecture</i>	281
14.1.2	<i>Phases for Start-Up of Relay Nodes</i>	283
14.2	Security Solution	284
14.2.1	<i>Security Concepts</i>	284
14.2.2	<i>Security Procedures</i>	288
14.2.3	<i>Security on the Un Interface</i>	290
14.2.4	<i>USIM and Secure Channel Aspects</i>	290
14.2.5	<i>Enrolment Procedures</i>	291
14.2.6	<i>Handling of Subscription and Certificates</i>	291
15	Security for Machine-Type Communications	293
15.1	Security for MTC at the Application Level	294
15.1.1	<i>MTC Security Framework</i>	295
15.1.2	<i>Security (Kmr) Bootstrapping Options</i>	298
15.1.3	<i>Connection (Kmc) and Application-Level Security Association (Kma) Establishment Procedures</i>	301
15.2	Security for MTC at the 3GPP Network Level	301
15.2.1	<i>3GPP System Improvements for MTC</i>	301
15.2.2	<i>Security Related to 3GPP System Improvements for MTC</i>	303