

ETSI TS 133 320 V14.0.0 (2017-05)



**Universal Mobile Telecommunications System (UMTS);
LTE;
Security of Home Node B (HNB)
/ Home evolved Node B (HeNB)
(3GPP TS 33.320 version 14.0.0 Release 14)**



Reference

RTS/TSGS-0333320ve00

Keywords

LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.

All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	6
1 Scope	7
2 References	7
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	8
4 Overview of Security Architecture and Requirements.....	9
4.1 System architecture of H(e)NB	9
4.2 Network Elements	10
4.2.1 H(e)NB	10
4.2.2 Security Gateway (SeGW).....	10
4.2.3 H(e)NB Management System (H(e)MS)	11
4.2.4 UE.....	11
4.2.5 H(e)NB Gateway (H(e)NB-GW) and MME.....	11
4.2.6 AAA Server and HSS	11
4.2.7 Void	11
4.2.8 Local Gateway (L-GW)	11
4.3 Interfaces (Reference Points)	11
4.3.1 Backhaul Link.....	11
4.3.2 H(e)MS Interface	11
4.3.3 Interface between SeGW and AAA Server, AAA Server and HSS.....	11
4.3.4 Interface between H(e)NBs.....	12
4.4 Security Requirements and Principles.....	12
4.4.1 Operation	12
4.4.2 Requirements on H(e)NB	12
4.4.3 Requirements on SeGW.....	13
4.4.4 Requirements on H(e)MS	13
4.4.5 Requirements on Backhaul Link.....	14
4.4.6 Requirements on H(e)MS Link.....	14
4.4.7 Requirements on Local Gateway (L-GW)	15
4.4.8 Requirements on the Direct Link between H(e)NBs	15
4.4.9 Requirements on Verification of H(e)NB Identity and Operating Access Mode.....	15
5 Security Features	16
5.1 Secure Storage and Execution.....	16
5.1.1 Hosting Party Module.....	16
5.1.2 Trusted Environment (TrE).....	16
5.1.2.1 General	16
5.2 Device Mutual Authentication	17
5.3 Hosting Party Mutual Authentication.....	17
5.4 Other security features.....	18
6 Security Procedures in H(e)NB	19
6.1 Device Integrity Check.....	19
6.1.1 Device Integrity Check Procedure	19
6.1.2 Protection of Trusted Reference Value(s).....	19
6.2 Void.....	19
6.3 Measures for Clock Protection	19
6.3.1 Clock Synchronization Security Mechanisms for H(e)NB	19
7 Security Procedures between H(e)NB and SeGW	20
7.1 Device Validation.....	20

7.2	Device Authentication	20
7.2.1	General	20
7.2.2	SeGW and Device Mutual Authentication Procedure	21
7.2.3	H(e)NB/IKEv2 Processing Requirements for SeGW Certificates	22
7.2.4	SeGW/IKEv2 Processing Requirements for H(e)NB Certificates	22
7.2.5	Security Profiles	22
7.2.5.1	Profile for IKEv2	22
7.2.5.2	IKEv2 Certificate Profile	23
7.2.5.2.1	IKEv2 Entity Certificates	23
7.2.5.2.2	IKEv2 CA Certificates	23
7.3	Hosting Party Authentication	23
7.4	IPsec Tunnel Establishment	24
7.5	Device Authorization	24
8	Security Aspects of H(e)NB Management	25
8.1	Location Verification	25
8.1.1	General	25
8.1.2	IP Address provided by H(e)NB	25
8.1.3	IP Address and/or access line location identifier provided by broadband access provider	25
8.1.4	Surrounding macro-cell information provided by H(e)NB	25
8.1.5	GNSS information provided by H(e)NB	25
8.1.6	Requirements	26
8.2	Access Control Mechanisms for H(e)NB	26
8.2.1	Non-CSG Method	26
8.2.2	CSG Method	26
8.3	Protection of H(e)MS traffic between H(e)MS and H(e)NB	26
8.3.1	Connection to H(e)MS accessible on MNO Intranet	26
8.3.2	Connection to H(e)MS accessible on public Internet	27
8.3.2.1	General	27
8.3.2.2	Device Validation	27
8.3.3	TLS certificate profile	28
8.3.3.1	TLS entity certificates	28
8.3.3.2	TLS CA certificates	28
8.3.4	TR-069 protocol profile	29
8.4	Protection of SW Download	29
8.5	Enrolment of H(e)NB to an Operator PKI	30
8.5.1	General	30
8.5.2	Enrolment Procedure	30
8.5.3	Certificate Validation	30
9	Security Aspects of Emergency Call Handling	31
10	Security Aspects for Mobility	32
10.1	Inbound mobility	32
10.2	Outbound mobility	32
11	Security Procedures for Direct Interfaces between Base Stations	33
11.1	General	33
11.2	Direct Link between two H(e)NBs	33
	Annex A (informative): Authentication Call-flows	34
A.1	Device Authentication Call-flow Example	34
A.2	Combined Device and HP Authentication Call-flow Example	35
	Annex B (informative): Location Verification Examples	38
B.1	Example of Location verification based on IP address and line identifier in NASS	38
B.2	Example process of location verification when the verifying node receive different types of location information	38
	Annex C: Change history	40

History42

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the security architecture for the H(e)NB subsystem. This includes security requirements on Home Node Bs, Home eNode Bs, and other H(e)NB-associated network nodes (e.g. SeGW and H(e)MS), as well as the procedures and features which are provided to meet those requirements.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

For a specific reference, subsequent revisions do not apply.

For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 32.583: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS) ".
- [3] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) ".
- [4] - [5] Void.
- [6] IETF RFC 4739: "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2 Protocol", Nov 2006".
- [7] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF) ".
- [8] 3GPP TS 23.003: "Numbering, addressing and identification".
- [9] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [10] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".
- [11] 3GPP TS 32.593: "Telecommunication management; Procedure flows for Type 1 interface H(e)NB to H(e)NB Management System (H(e)MS) ".
- [12] 3GPP TS 25.467: "UTRAN architecture for 3G Home Node B (HNB); Stage 2".
- [13] - [14] Void.
- [15] The Broadband Forum TR-069: "CPE WAN Management Protocol v1.1", Issue 1 Amendment 2, December 2007.
- [16] - [17] Void.
- [18] ETSI ES 282 004 (V1.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN functional architecture; Network Attachment Sub-System (NASS) ", 2006.
- [19] ETSI ES 283 035 (V1.1.1): "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol", 2006.
- [20] 3GPP TS 33.102: "3G security; Security architecture".