

ETSI TS 133 320 V9.7.0 (2013-02)



**Universal Mobile Telecommunications System (UMTS);
LTE;
Security of Home Node B (HNB)
/ Home evolved Node B (HeNB)
(3GPP TS 33.320 version 9.7.0 Release 9)**

[ETSI TS 133 320 V9.7.0 \(2013-02\)](https://standards.iteh.ai/catalog/standards/etsi/4224451a-f881-4b32-9c13-35eac5624760/etsi-ts-133-320-v9-7-0-2013-02)

<https://standards.iteh.ai/catalog/standards/etsi/4224451a-f881-4b32-9c13-35eac5624760/etsi-ts-133-320-v9-7-0-2013-02>



Reference

RTS/TSGS-0333320v970

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

(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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

<http://portal.etsi.org/tb/status/status.asp>

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

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2013.
All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
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 (<http://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>.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 133 320 V9.7.0 \(2013-02\)](https://standards.iteh.ai/catalog/standards/etsi/4224451a-f881-4b32-9c13-35eac5624760/etsi-ts-133-320-v9-7-0-2013-02)

<https://standards.iteh.ai/catalog/standards/etsi/4224451a-f881-4b32-9c13-35eac5624760/etsi-ts-133-320-v9-7-0-2013-02>

Contents

Intellectual Property Rights	2
Foreword.....	2
Foreword.....	5
1 Scope	6
2 References	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	7
4 Overview of Security Architecture and Requirements.....	8
4.1 System architecture of H(e)NB	8
4.2 Network Elements	9
4.2.1 H(e)NB	9
4.2.2 Security Gateway (SeGW).....	9
4.2.3 H(e)NB Management System (H(e)MS)	9
4.2.4 UE	9
4.2.5 H(e)NB Gateway (H(e)NB-GW) and MME.....	9
4.2.6 AAA Server and HSS	10
4.2.7 Void	10
4.3 Interfaces (Reference Points)	10
4.3.1 Backhaul Link.....	10
4.3.2 H(e)MS Interface	10
4.3.3 Interface between SeGW and AAA Server, AAA Server and HSS.....	10
4.4 Security Requirements and Principles.....	10
4.4.1 Operation	10
4.4.2 Requirements on H(e)NB	10
4.4.3 Requirements on SeGW.....	11
4.4.4 Requirements on H(e)MS	11
4.4.5 Requirements on Backhaul Link.....	12
4.4.6 Requirements on H(e)MS Link.....	12
5 Security Features	13
5.1 Secure Storage and Execution	13
5.1.1 Hosting Party Module	13
5.1.2 Trusted Environment (TrE).....	13
5.1.2.1 General	13
5.2 Device Mutual Authentication	13
5.3 Hosting Party Mutual Authentication.....	14
5.4 Other security features.....	14
6 Security Procedures in H(e)NB.....	15
6.1 Device Integrity Check.....	15
6.1.1 Device Integrity Check Procedure	15
6.1.2 Protection of Trusted Reference Value(s).....	15
6.2 Void.....	15
6.3 Measures for Clock Protection	15
6.3.1 Clock Synchronization Security Mechanisms for H(e)NB	15
7 Security Procedures between H(e)NB and SeGW	16
7.1 Device Validation.....	16
7.2 Device Authentication	16
7.2.1 General.....	16
7.2.2 SeGW and Device Mutual Authentication Procedure.....	16
7.2.3 H(e)NB/IKEv2 Processing Requirements for SeGW Certificates	18
7.2.4 SeGW/IKEv2 Processing Requirements for H(e)NB Certificates	18

7.2.5	Security Profiles.....	18
7.2.5.1	Profile for IKEv2	18
7.2.5.2	IKEv2 Certificate Profile	19
7.2.5.2.1	IKEv2 Entity Certificates	19
7.2.5.2.2	IKEv2 CA Certificates	19
7.3	Hosting Party Authentication	19
7.4	IPsec Tunnel Establishment	20
7.5	Device Authorization	20
8	Security Aspects of H(e)NB Management.....	21
8.1	Location Verification	21
8.1.1	General.....	21
8.1.2	IP Address provided by H(e)NB.....	21
8.1.3	IP Address and/or access line location identifier provided by broadband access provider.....	21
8.1.4	Surrounding macro-cell information provided by H(e)NB.....	21
8.1.5	GNSS information provided by H(e)NB	21
8.1.6	Requirements	22
8.2	Access Control Mechanisms for H(e)NB	22
8.2.1	Non-CSG Method.....	22
8.2.2	CSG Method	22
8.3	Protection of H(e)MS traffic between H(e)MS and H(e)NB.....	22
8.3.1	Connection to H(e)MS accessible on MNO Intranet	22
8.3.2	Connection to H(e)MS accessible on public Internet	23
8.3.2.1	General	23
8.3.2.2	Device Validation	23
8.3.3	TLS certificate profile.....	24
8.3.3.1	TLS entity certificates.....	24
8.3.3.2	TLS CA certificates.....	24
8.3.4	TR-069 protocol profile	24
8.4	Protection of SW Download.....	25
9	Security Aspects of Emergency Call Handling.....	25
10	Security Aspects for Mobility	27
10.1	Inbound mobility	27
10.2	Outbound mobility	27
Annex A (informative):	Authentication Call-flows.....	28
A.1	Device Authentication Call-flow Example	28
A.2	Combined Device and HP Authentication Call-flow Example	29
Annex B (informative):	Location Verification Examples	32
B.1	Example of Location verification based on IP address and line identifier in NASS.....	32
B.2	Example process of location verification when the verifying node receive different types of location information	32
Annex C:	Change history	34
History		35