

# ETSI TS 133 320 V18.0.0 (2024-04)



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
Security of Home Node B (HNB)  
/ Home evolved Node B (HeNB)  
(3GPP TS 33.320 version 18.0.0 Release 18)**

[ETSI TS 133 320 V18.0.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/c9f44bd0-8b67-4a82-ab18-4842d4924e46/etsi-ts-133-320-v18-0-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/c9f44bd0-8b67-4a82-ab18-4842d4924e46/etsi-ts-133-320-v18-0-0-2024-04>



---

**Reference**

RTS/TSGS-0333320v100

---

**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 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from:

<https://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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**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.

© ETSI 2024.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

## Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables. (2024-04)

The cross reference between 3GPP and ETSI identities can be found under <https://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
Legal Notice .....	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
<b>Annex A (informative):</b>	<b>Authentication Call-flows.....</b>	<b>34</b>
A.1	Device Authentication Call-flow Example .....	34
A.2	Combined Device and HP Authentication Call-flow Example .....	35
<b>Annex B (informative):</b>	<b>Location Verification Examples .....</b>	<b>38</b>
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
<b>Annex C:</b>	<b>Change history .....</b>	<b>40</b>

History .....42

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

[ETSI TS 133 320 V18.0.0 \(2024-04\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/c9f44bd0-8b67-4a82-ab18-4842d4924e46/etsi-ts-133-320-v18-0-0-2024-04>

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> 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.

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

[ETSI TS 133 320 V18.0.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/c9f44bd0-8b67-4a82-ab18-4842d4924e46/etsi-ts-133-320-v18-0-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/c9f44bd0-8b67-4a82-ab18-4842d4924e46/etsi-ts-133-320-v18-0-0-2024-04>

---

# 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".

- [21] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE): Security architecture".
- [22] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"
- [23] Open Mobile Alliance OMA-WAP-OCSP V1.0: "Online Certificate Status Protocol Mobile Profile". URL: <http://www.openmobilealliance.org/>
- [24] IETF RFC 4806: "Online Certificate Status Protocol (OCSP) Extensions to IKEv2".
- [25] Void.
- [26] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [27] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".
- [28] 3GPP TS 25.367: "Mobility procedures for Home Node B (HNB); Overall description; Stage 2".
- [29] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [30] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [31] 3GPP TS 22.220: "Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**CSG:** A closed subscriber group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN of but having restricted access ("CSG cells")

**Hosting party:** The party hosting the H(e)NB and having a contract with the PLMN operator.

**Security Gateway:** Element at the edge of an operator's security domain terminating security association(s) for the backhaul link between H(e)NB and network.

### 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACS	Auto-Configuration Server
AKA	Authentication and Key Agreement
CA	Certification Authority
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CSG	Closed Subscriber Group
DNS	Domain Name System
DPD	Dead Peer Detection
eNB	Evolved Node-B
EAP	Extensible Authentication Protocol

ESP	Encapsulating Security Payload
E-UTRAN	Evolved UTRAN
FQDN	Fully Qualified Domain Name
GNSS	Global Navigation Satellite System
H(e)NB	Home NodeB or Home eNodeB
H(e)NB-GW	Home (e)NodeB Gateway
H(e)MS	Home NodeB Management or Home eNodeB Management System
HeMS	Home eNodeB Management System
HeNB	Home eNodeB
HMS	Home NodeB Management System
HNB	Home NodeB
HP	Hosting Party
HPM	HP Module
HW	Hardware
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
L-GW	Local Gateway
LIPA	Local IP Access
LTE	Long Term Evolution
MME	Mobility Management Entity
MSK	Master Session Key
NAPT	Network Address Port Translation
NAT	Network Address Translation
NAT-T	NAT-Traversal
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SA	Security Association
SeGW	Security Gateway
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
TLS	Transport Layer Security
TrE	Trusted Environment
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network
WAP	Wireless Application Protocol

## 4 Overview of Security Architecture and Requirements

### 4.1 System architecture of H(e)NB

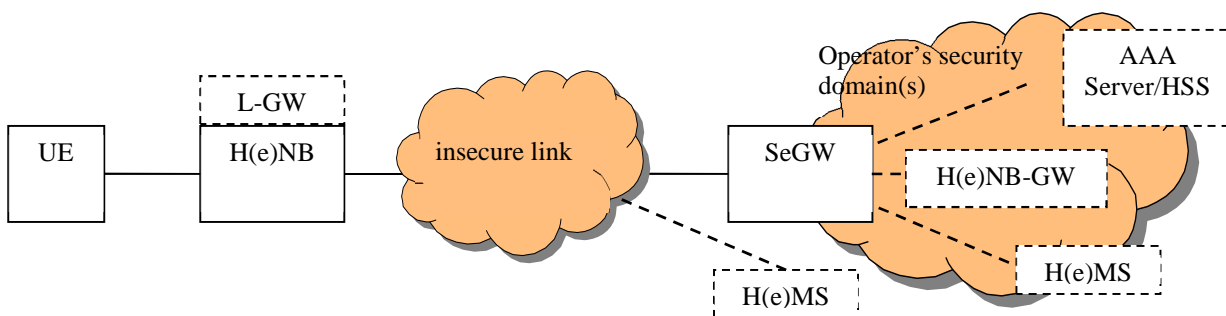


Figure 4.1.1: System Architecture of H(e)NB

Description of the system architecture:

- Air interface between UE and H(e)NB should be backwards compatible to the air interface in UTRAN or E-UTRAN.
- H(e)NB accesses the operator's security domain via a Security Gateway (SeGW). The backhaul between H(e)NB and SeGW may be insecure.
- Security Gateway represents the operator's core network with respect to performing mutual authentication with the H(e)NB.
- AAA server authenticates the hosting party based on the authentication information retrieved from HSS when hosting party authentication is performed.
- Security tunnel is established between H(e)NB and Security Gateway to protect information transmitted in backhaul link.
- HNB-GW performs mandatory UE access control and HNB performs optional UE access control in the case of non-CSG capable UEs or non-CSG capable HNBs. SeGW and HNB-GW are logically separate entities within operator's network, with the SeGW located in front of the HNB-GW. The SeGW may be integrated into the HNB-GW. If the SeGW and the HNB-GW are not integrated, then the interface between the HNB-GW and the SeGW may be protected using NDS/IP as specified in TS 33.210 [9]. The interface between HNB-GW and MSC/SGSN may be protected using NDS/IP.
- HeNB-GW is optional to deploy. When HeNB-GW is not deployed, the SeGW is located at the edge of the core network and the interface between SeGW and MME/S-GW may be protected using NDS/IP as specified in TS 33.210 [9]. When HeNB-GW is deployed, then SeGW and HeNB-GW are logically separate entities, with the SeGW located in front of the HeNB-GW. The SeGW may be integrated into HeNB-GW. If the SeGW and the HeNB-GW are not integrated, then the interface between the HeNB-GW and the SeGW may be protected using NDS/IP, the interface between HeNB-GW and MME/S-GW may be protected using NDS/IP.
- HMS as specified in TS 32.583 [2] and/or HNB-GW as specified in TS 25.467 [12] performs location verification of HNB.
- HeMS as specified in TS 32.593 [11] performs location verification of HeNB.
- Secure communication is required to H(e)NB Management System (H(e)MS).
- L-GW is optional to deploy. If L-GW is deployed, then the secured interface between H(e)NB and Security Gateway is used by the L-GW to communicate with the core network.

## 4.2 Network Elements

### 4.2.1 H(e)NB

The H(e)NB is a network element that connects User Equipment via its radio interface to the operator's core network. The backhaul link to the operator's network is a broadband connection. A H(e)NB is typically deployed in customers' premises.

**NOTE:** The term H(e)NB refers to both Home NodeB (HNB) and Home eNodeB (HeNB), when both are meant without distinction.

### 4.2.2 Security Gateway (SeGW)

The SeGW is a network element at the border of a security domain of the operator. If a H(e)NB-GW is deployed the SeGW is located in front of the H(e)NB-GW, else it is located at the edge of the core network. After successful mutual authentication between the H(e)NB and the SeGW, the SeGW connects the H(e)NB to the operator's security domain. Any connection between the H(e)NB and the H(e)NB-GW or core network is tunnelled through the SeGW.

### 4.2.3 H(e)NB Management System (H(e)MS)

The H(e)MS is a management server that configures the H(e)NB according to the operator's policy. H(e)MS is also capable of installing software updates on the H(e)NB. The H(e)MS server may be located inside the operator's access or core network (accessible on the MNO Intranet) or outside of it (accessible on the public Internet).

The HMS is specified in TS 32.583 [2].

The HeMS is specified in TS 32.593 [11].

### 4.2.4 UE

UE is a standard user equipment for UMTS (for HNB) or LTE (for HeNB).

### 4.2.5 H(e)NB Gateway (H(e)NB-GW) and MME

HNB-GW is specified in TS 25.467 [12] and HeNB-GW is specified in TS 36.300 [27].

### 4.2.6 AAA Server and HSS

HSS stores the subscription data and authentication information of the H(e)NBs. When hosting party authentication is required, AAA server authenticates the hosting party based on the authentication information retrieved from HSS.

### 4.2.7 Void

### 4.2.8 Local Gateway (L-GW)

L-GW is specified in TS 23.060 [29] and in TS 23.401 [30]. The Local IP Access (LIPA) is achieved using a L-GW colocated with the H(e)NB. The L-GW is connected to the Serving Gateway (S-GW) or to the SGSN via the SeGW.

## 4.3 Interfaces (Reference Points)

### 4.3.1 Backhaul Link

The backhaul link used between H(e)NB and SeGW provides a secure tunnel carrying both the user plane data and the control plane data that are transmitted between the H(e)NB and the H(e)NB-GW or network elements in the core network.

**NOTE:** If LIPA is activated, the secured backhaul link between the H(e)NB and SeGW is used by the L-GW to communicate with the core network.

H(e)MS traffic is also tunnelled through this secure backhaul link, if the H(e)MS is accessible on the MNO Intranet.

The backhaul link may also carry other data between H(e)NB and operator's radio access or core network, e.g. time protocol traffic.

### 4.3.2 H(e)MS Interface

The H(e)MS Interface between the H(e)NB and the H(e)MS server shall provide a secure connection carrying configuration data, SW updates and additional data, e.g. location information.

### 4.3.3 Interface between SeGW and AAA Server, AAA Server and HSS

The interface between the SeGW and AAA Server provides a secure connection carrying authentication, authorization, and related information.