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)

Reference
RTS/TSGS-0333320vi00

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

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.

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

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".

[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

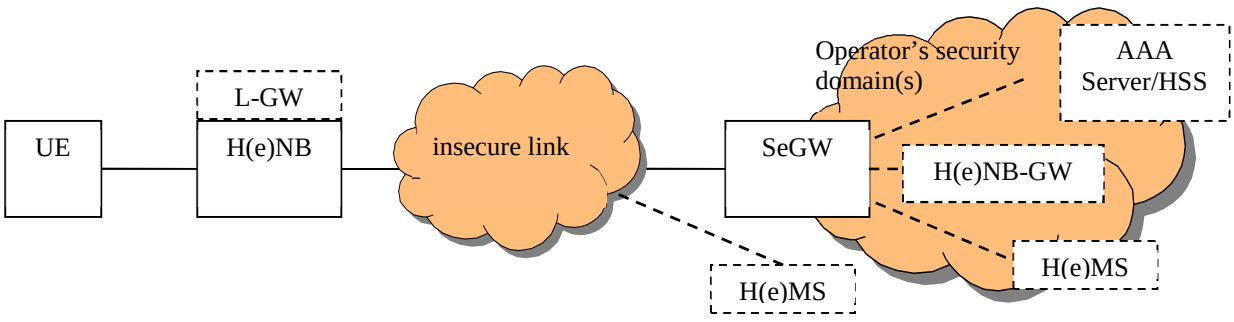

Figure 4.1.1: System Architecture of H(e)NB

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.