



**Universal Mobile Telecommunications System (UMTS);  
LTE;  
Telecommunication management;  
Home Node B (HNB) Operations, Administration,  
Maintenance and Provisioning (OAM&P);  
Concepts and requirements for Type 1 interface HNB to HNB  
Management System (HMS)  
(3GPP TS 32.581 version 15.0.0 Release 15)**



---

Reference

RTS/TSGS-0532581vf00

---

Keywords

LTE,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.

© ETSI 2018.

All rights reserved.

**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 protected for the benefit of its Members.

**GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables 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.

## 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.

---

# 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.....                                      | 4         |
| Introduction .....                                 | 4         |
| 1 Scope .....                                      | 5         |
| 2 References .....                                 | 5         |
| 3 Definitions and abbreviations.....               | 5         |
| 3.1 Definitions .....                              | 5         |
| 3.2 Abbreviations .....                            | 5         |
| 4 Concepts and background .....                    | 6         |
| 5 Business level requirements .....                | 6         |
| 5.1 Requirements.....                              | 6         |
| 5.1.1 Configuration Management .....               | 6         |
| 5.1.2 Performance Management .....                 | 6         |
| 5.1.3 Fault Management .....                       | 7         |
| 5.1.4 Security Management .....                    | 7         |
| 5.2 Actor roles .....                              | 7         |
| 5.3 Telecommunications resources .....             | 7         |
| 5.4 High level use cases .....                     | 7         |
| 6 Specification level requirements .....           | 7         |
| 6.1 Requirements.....                              | 7         |
| 6.1.1 Configuration Management .....               | 7         |
| 6.1.2 Performance Management .....                 | 8         |
| 6.1.3 Fault Management .....                       | 8         |
| 6.1.4 Security Management .....                    | 9         |
| 6.2 Actor roles .....                              | 10        |
| 6.3 Telecommunications resources .....             | 10        |
| 6.4 Use cases .....                                | 10        |
| <b>Annex A (informative): Change history .....</b> | <b>11</b> |
| History .....                                      | 12        |

---

# 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.

---

# Introduction

The present document is part of a TS-family covering the 3<sup>rd</sup> Generation Partnership Project Technical Specification Group Services and System Aspects, Telecommunication Management; as identified below:

**3GPP TS 32.581: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Concepts and requirements for Type 1 interface HNB to HNB Management System (HMS)".**

3GPP TS 32.582: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HNB to HNB Management System (HMS)".

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)".

3GPP TS 32.584: "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); XML definitions for Type 1 interface HNB to HNB Management System (HMS)".

---

# 1 Scope

The present document describes the concepts and requirements of OAM for Home NodeB (HNB). The requirements captured in this document shall be met via Type 1 interface between HNB and HMS.

---

## 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 32.821: "Study of Self-Organizing Network (SON) related OAM for Home NodeB".
  - [2] 3GPP TS 25.467: "UTRAN architecture for 3G Home NodeB, stage 2".
  - [3] TR-069 Amendment 2, CPE WAN Management Protocol v1.1, Broadband Forum
  - [4] TR-106 Amendment 2 Data Model template for TR-069-Enabled Devices v1.1, Broadband Forum.
  - [5] TR-196 FAP Access Point Service Data Model v1.00, Broadband Forum.
  - [6] 3GPP TS 32.435: "Performance Measurement, eXtensible Markup Language (XML) file format definition".
  - [7] 3GPP TS 32.111-2: "Telecommunication management; Fault Management; Alarm Integration Reference Point (IRP): Information Service (IS)".
  - [8] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".
  - [9] 3GPP TS 32.102: "Telecommunication management; Architecture".
  - [10] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
  - [11] 3GPP TS 22.220: "Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".
  - [12] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".
- 

## 3 Definitions and abbreviations

For the purposes of the present document, the terms and definitions given in TS 32.101 [8], TS 32.102 [9] and TS 21.905 [10] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TS 32.101 [8], TS 32.102 [9] and TS 21.905 [10], in that order.

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [10] 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 [10].

### 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

|     |                              |
|-----|------------------------------|
| HMS | Home NodeB Management System |
| HNB | Home NodeB                   |

---

## 4 Concepts and background

Home NodeB has the following characteristics:

- The quantity of Home NodeBs is likely to be large
- There may be many Home NodeB vendors
- Home NodeB may be purchased easily by end users in market
- The location of Home NodeB could be in a private residence which may not be accessible for frequent on-site maintenance

Based on the above characteristics, this specification defines the functionalities needed for the management of Home NodeB over a Type 1 interface.

---

## 5 Business level requirements

### 5.1 Requirements

**REQ-OAMP-CON-001** The HNB shall be able to be managed in all management domain aspects defined below as Configuration management, Security management, Performance management and Fault management, without the use of vendor-specific or operator-specific extension capability.

#### 5.1.1 Configuration Management

**REQ-OAMP\_CM-CON-001** The HNB shall be able to automatically, i.e. without human operator on-line interaction or attention, configure itself to be ready for service when powered up and connected to HMS.

**REQ-OAMP\_CM-CON-002** The HNB shall be able to automatically, i.e. without human operator on-line interaction or attention, configure itself to be in service when powered up and connected to HMS.

**REQ-OAMP\_CM-CON-003** The HNB shall be able to automatically, i.e. without human operator on-line interaction or attention, upgrade its software/firmware and configuration.

**REQ-OAMP\_CM-CON-004** The HNB auto-configuration shall be done in such way that the performance of the surrounding macro cells is not adversely affected.

**REQ-OAMP\_CM-CON-005** The HNB auto-configuration function should be adaptive to react to change in the network and changes in the radio environment.

**REQ-OAMP\_CM-CON-006** The operator shall be able to remotely reboot the HNB.

**REQ-OAMP\_CM-CON-007** The operator shall be able to remotely start/stop the radio transmission of the HNB.

**REQ-OAMP\_CM-CON-008** In case IPsec is used, the system should be engineered to ensure that the HNB IP address changes as minimally as possible.

**REQ-OAMP\_CM-CON-009** The operator shall be able to remotely reconfigure the HNB to adapt to changes in the radio environment.

**REQ-OAMP\_CM-CON-010** The HNB should allow configuration of the IPsec or non-IPsec usage option based on the operator's policy TS 33.320 [12].

#### 5.1.2 Performance Management

**REQ-OAMP\_PM-CON-001** The HNB may have the capability to collect its performance related data.

**REQ-OAMP\_PM-CON-002** The HNB shall send performance data based on operator configured policy.

**REQ-OAMP\_PM-CON-003** Operator shall be able to retrieve performance data file from the HNB.

### 5.1.3 Fault Management

**REQ-OAMP\_FM-CON-001** The HNB shall support Fault Management to enable the operator to monitor and manage the HNB.

**REQ-OAMP\_FM-CON-002** The HNB shall provide alarm related information only on demand by the operator or based on operator configured policy.

### 5.1.4 Security Management

**REQ-OAMP\_SM-CON-001** The HNB shall have the capability to protect itself against Denial of Service attack over the Type 1 interface.

## 5.2 Actor roles

Not defined in this version.

## 5.3 Telecommunications resources

Not defined in this version.

## 5.4 High level use cases

Not defined in this version.

---

# 6 Specification level requirements

## 6.1 Requirements

### 6.1.1 Configuration Management

The requirements for configuration management are as follows:

**REQ-OAMP\_CM-FUN-001** The HNB configuration shall be administered by the HMS utilising the TR-069 CWMP Protocol, reference [3].

**REQ-OAMP\_CM-FUN-002** The HNB Information Model used by the HMS for Configuration Management shall be based on the following:

- a. Broadband Forum TR-106 Amendment 2 Data Model [4]
- b. FAP Access Point Service Data Model [5]

**REQ-OAMP\_CM-FUN-003** HMS shall be able to reboot the HNB.

**REQ-OAMP\_CM-FUN-004** HMS shall have remote access to the HNB to start/stop the radio transmission.

**REQ-OAMP\_CM-FUN-005** HMS shall have remote access to the HNB to start/stop the radio transmission on the frequencies specified by HMS.

**REQ-OAMP\_CM-FUN-006** HMS shall maintain the configuration data of the HNB.

**REQ-OAMP\_CM-FUN-007** When the HNB is initially powered up and connected to the HMS, HMS shall send the initially needed configuration data to the HNB.

**REQ-OAMP\_CM-FUN-008** If the inner IPsec tunnel IP address of the HNB changes and HNB is connected to HMS via IPsec Tunnel then the HNB shall notify the HMS using TR-069.

**REQ-OAMP\_CM-FUN-009** The HMS shall specify which parameters it needs to be notified of when the HNB changes their values through auto-configuration. The HNB shall notify the HMS of changes in the values of any such auto-configured parameters.



**REQ-OAMP\_CM-FUN-010** The HNB shall inform the HMS of its ability to auto-configure parameters or groups of parameters that are relevant to the HMS.

**REQ-OAMP\_CM-FUN-011** HMS shall be able to specify a value, or a valid range of values, for any parameter that is auto-configurable by the HNB.

**REQ-OAMP\_CM-FUN-012** Configuration management capability for the HNB shall be supported by means of TR-069 RPCs SetParameterValues, AddObject and DeleteObject. Optionally a bulk configuration management file may be supported. In this case the TR-069 manager uses the RPC download method to trigger a CM file download from a file server.

**REQ-OAMP\_CM-FUN-013** The HNB shall be able to inform the HMS of the changes in radio environment.

**REQ-OAMP\_CM-FUN-014** The HNB shall provide a capability allowing the HMS to manage downloading of HNB software/firmware image files and provide mechanisms for version identification and notification to the HMS of the success or failure of a file download.

**REQ-OAMP\_CM-FUN-015** The HNB shall support capabilities to inform the HMS about the results of specific actions triggered by the HMS.

**REQ-OAMP\_CM-FUN-016** It shall be possible to initiate a management connection at the request of either the HNB or the HMS.

**REQ-OAMP\_CM-FUN-017** If the HNB is unable to offer service for an operator configured time period it will deactivate the air interfac.

**REQ-OAMP\_CM-FUN-018** The HNB shall support a capability to allow the HMS to activate Local IP Access.

**REQ-OAMP\_CM-FUN-019** The HNB shall support a capability to allow the HMS to deactivate Local IP Access.

**REQ-OAMP\_CM-FUN-020** The HMS should be able to securely configure the HNB according to the operator's policy, whether or not to use IPsec for subsequent connections.

## 6.1.2 Performance Management

The HNB may support Performance Management to enable the operator to monitor the HNB Network based on the business level requirements (see clause 5.1.2).

The requirements for performance management are as follows.

**REQ-OAMP\_PM-FUN-001** The HNB may have the Performance Management capabilities administered by the HMS.

**REQ-OAMP\_PM-FUN-002** The HNB shall support the retrieval of the Performance Information from the HNB utilising the file transfer option of TR-069 CWMP Protocol, reference [3].

**REQ-OAMP\_PM-FUN-003** The HNB shall be configurable by the HMS to produce an XML File at regular intervals which contains the HNB performance Information and then upload the XML File.

**REQ-OAMP\_PM-FUN-004** The XML File Formats produced by the HNB shall adhere to the 3GPP XML Performance Management File Formats, reference [6].

**REQ-OAMP\_PM-FUN-005** The HNB shall upload PM files using TR-069 compliant file transfer protocols.

**REQ-OAMP\_PM-FUN-006** The HMS shall have the capability to initiate HNB diagnostic testing

**REQ-OAMP\_PM-FUN-007** HMS shall have the ability to configure policies for the HNB performance data file upload.

## 6.1.3 Fault Management

**REQ-OAMP\_FM-FUN-001** The HNB shall have the Fault Management capabilities administered through the HMS.

**REQ-OAMP\_FM-FUN-002** The HNB shall have the ability to send alarm related information to HMS according to operator configured policy.

**REQ-OAMP\_FM-FUN-003** The HNB shall be able to send alarm related information to the HMS using TR-069 RPC Methods, reference [3].

**REQ-OAMP\_FM-FUN-004** The alarm related information to be sent to the HMS by the HNB shall support the inclusion of the appropriate Information attributes, as defined in 3GPP TS.32.111-2, reference [7].

**REQ-OAMP\_FM-FUN-005** The HNB shall maintain the following information:

- a. Alarm Management Information – which contains the alarm management and reporting parameters configurable by the HMS
- b. Alarms List – Alarms currently active on the HNB
- c. Alarm History – contains the alarms previously created by the HNB.
- d. Pending Delivery Queue – contains the alarms queued to be sent to the HMS on the next management connection

**REQ-OAMP\_FM-FUN-006.**The HNB shall support the following ways of alarm handling:

- a. Expedited handling– the HNB connects to the HMS immediately to raise the alarm and logs the alarm in the Alarm History.
- b. Queued handling – the HNB queues the alarm internally pending connection to the HMS, logs the alarm in the Alarm History, and delivers the alarm on the next connection to the HMS
- c. Logged handling – the HNB does not send the alarm to the HMS and logs the alarm in the Alarm History.
- d. Disabled handling– the HNB does not send the alarm to the HMS and will not log the alarm in the Alarm History

**REQ-OAMP\_FM-FUN-007** The HMS may configure the alarm handling for each type of HNB alarm according to the HNB alarm handling capabilities and the default handling if not specified by the HMS shall be “Logged handling”.

**REQ-OAMP\_FM-FUN-008** The HMS shall have the ability to throttle the sending of alarms from the HNB to the HMS

**REQ-OAMP\_FM-FUN-009** The HMS shall have the capability to retrieve alarm related information from the HNB using TR-069 RPC Method Calls.

**REQ-OAMP\_FM-FUN-010** The HMS shall have the capability to completely purge on the HNB the Alarms List and the Pending Delivery Queue and may have the capability to completely purge on the HNB the history of Alarms.

**REQ-OAMP\_FM-FUN-011** The HMS shall have the capability to activate and deactivate the alarm reporting by the HNB.

**REQ-OAMP\_FM-FUN-012** The HMS shall be able to define the frequency of passive reporting.

**REQ-OAMP\_FM-FUN-013** The HMS shall be informed immediately of alarms (raised, changed, cleared) classified as expedited notifications only.

**REQ-OAMP\_FM-FUN-014** The HNB shall provide a capability allowing the HMS to access information that it may use to diagnose and resolve connectivity or service issues.

## 6.1.4 Security Management

**REQ-OAMP\_SM-FUN-001.**The HNB shall have the capability to communicate with the HMS via TR-069 CWMP, reference [3], through the support of one of the two security mechanisms determined by the Network Operator’s Security Policies:

- utilising SSL/TLS outside the IPsec Tunnel
- within the IPsec Tunnel with the option to utilise SSL/TLS within the IPsec Tunnel for additional end-to-end security

TR-069 CPE devices are currently factory programmed with a Bootstrap HMS URL only and therefore the HNB capable CPEs requiring to utilise IPsec for connection to the HMS either require to be factory programmed with Bootstrap Security Gateway/IPsec Information or this information is supplied outside of the IPsec tunnel before tunnel establishment utilising SSL/TLS.

**REQ-OAMP\_SM-FUN-002** The HNB shall provide a capability to prevent tampering with the interactions that take place between the HNB and the HMS as well as management functions of a HNB.

**REQ-OAMP\_SM-FUN-003** The HNB shall provide a capability allowing the HMS to authenticate the HNBs.

**REQ-OAMP\_SM-FUN-004** The HNB shall be able to authenticate the HMS prior to responding to interactions triggered by the HMS.

**REQ-OAMP\_SM-FUN-005** The HNB shall provide a capability supporting confidentiality for interaction taking place between the HNB and the HMS.

## 6.2 Actor roles

Not defined in this version.

## 6.3 Telecommunications resources

Not defined in this version.

## 6.4 Use cases

Not defined in this version.

## Annex A (informative): Change history

| Change history |       |           |     |     |  |        |               |
|----------------|-------|-----------|-----|-----|--|--------|---------------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old    | New           |
| Mar 2009       | SP-43 | SP-090067 | --  | --  | Presentation to SA for information and approval  | 1.0.0  | 8.0.0         |
| Jun 2009       | SP-44 | SP-090295 | 001 | --  | Add requirements for HNB informing the HMS of the changes in radio environment                                   | 8.0.0  | 9.0.0         |
| Sep 2009       | SP-45 | SP-090534 | 003 | --  | Add missing description of AddObject and DeleteObject RPC method in configuration management according to BBF LS | 9.0.0  | 9.1.0         |
| Sep 009        | SP-45 | SP-090540 | 004 | --  | New CM, FM & SM specification level requirements for HNB Management  | 9.0.0  | 9.1.0         |
| Mar 2010       | SP-47 | SP-100035 | 006 | --  | Correction of file transfer mechanisms in HNB type 1 interface   | 9.1.0  | 9.2.0         |
| Jun 2010       | SP-48 | SP-100264 | 007 | --  | Missing Requirement for an operator's defined time period at the HNB   | 9.2.0  | 10.0.0        |
| Mar 2011       | SP-51 | SP-110099 | 008 | --  | Add LIPA management requirements   | 10.0.0 | 10.1.0        |
| May 2011       | SP-52 | SP-110288 | 010 | 2   | Correction of requirements for HNB non-IPsec usage - alignment with 33.320                                       | 10.1.0 | 10.2.0        |
| 2012-09        | -     | -         | -   | -   | Update to Rel-11 version (MCC)   | 10.2.0 | <b>11.0.0</b> |
| 2014-10        | -     | -         | -   | -   | Update to Rel-12 version (MCC)   | 11.0.0 | <b>12.0.0</b> |
| 2016-01        | -     | -         | -   | -   | Update to Rel-13 version (MCC)   | 12.0.0 | <b>13.0.0</b> |
| 2017-04        | SA#75 | -         | -   | -   | Promotion to Release 14 without technical change   | 13.0.0 | <b>14.0.0</b> |
| 2018-06        | -     | -         | -   | -   | Update to Rel-15 version (MCC)   | 14.0.0 | <b>15.0.0</b> |

---

# History

| <b>Document history</b> |           |             |
|-------------------------|-----------|-------------|
| V15.0.0                 | July 2018 | Publication |
|                         |           |             |
|                         |           |             |
|                         |           |             |
|                         |           |             |