ETSI TS 122 220 V16.0.0 (2020-08)

TECHNICAL SPECIFICATION

Universal Mobile Telecommunications System (UMTS);
Service requirements for Home Node B (HNB)
and Home eNode B (HeNB)
(3GPP TS 22.220 version 16.0.0 Release 16)

Reference

RTS/TSGS-0122220vg00

Keywords

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at 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/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

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.

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 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

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.

Introduction

In Rel-8, 3GPP has specified the basic functionalities for the support of Home Node B (HNB) and Home eNodeB (HeNB). The requirements for these basic functionalities were captured in TS 22.011.

From Rel-9 onward, it has been agreed to consolidate all the requirements from Rel-8 and further requirements for HNB and HeNB in a new TS, which is this specification.

1 Scope

This specification defines the service requirements for the basic functionalities for the support of Home NodeB (HNB) and Home eNodeB (HeNB) – jointly referred to as H(e)NB – and the further functionalities that will enable the mobile operators to provide more advanced services as well as improving the user experience.

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]   Void

[3]   3GPP TS 22.246: "Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1".

[4]   3GPP TS 22.101: "Service Aspects; Service Principles".

[5]   TR-069 Amendment 2: "CPE WAN Management Protocol v1.1, Broadband Forum", viewable at http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf

[6]   3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

[7]   3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[8]   3GPP TS 22.115: "Service aspects; Charging and billing".

[9]   3GPP TS 22.268: "Public Warning System (PWS) requirements".

[10]   3GPP TS 22.011: "Service accessibility".

[11]   3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Mobule (U)SIM Toolkit applications".

[12]   3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications".

3 Definitions, symbols 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].

Closed access mode: H(e)NB provides services only to its associated CSG members.

Home based network: An IP based network in the same premises as, and is connected to, the H(e)NB.

Hybrid access mode: H(e)NB provides services to its associated CSG members and to non-CSG members.

Open access mode: H(e)NB operates as a normal NodeB or eNodeB.

HNB: A HNB is a Customer-premises equipment that connects a 3GPP UE over UTRAN wireless air interface to a mobile operator's network using a broadband IP backhaul.

HeNB: A HeNB is a Customer-premises equipment that connects a 3GPP UE over EUTRAN wireless air interface to a mobile operator's network using a broadband IP backhaul.

H(e)NB Gateway: H(e)NB Gateway is a mobile operator's equipment (usually physically located on mobile operator premises) through which the H(e)NB gets access to mobile operator's core network.

H(e)NB Hosting Party: A H(e)NB Hosting Party has a contractual relationship with the operator, related to the provision of access to the operator's network via one or more H(e)NBs.

NOTE: A H(e)NB Hosting Party is likely to have the billing relationship with the operator. A H(e)NB Hosting Party will typically be the "lead" user in a household but could be e.g. the corporate IT manager in an enterprise context.

H(e)NB Subsystem: A H(e)NB Subsystem consists of the H(e)NB and the H(e)NB Gateway.

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].

CSG   Closed Subscriber Group

HNB   Home NodeB

HeNB   Home eNodeB

H(e)NB   HNB and HeNB

4 General

4.1 Description

Access to 3G and evolved 3G (EPS) services may be provided via UTRAN or E-UTRAN cellular base stations belonging to e.g. domestic, business, commercial enterprises. This type of access may be provided by the PLMN by means of HNB and HeNB (jointly referred to as H(e)NB). The H(e)NB provides services either only to a Closed Subscriber Group (CSG) or to other mobile subscribers too. The H(e)NB is connected to the mobile operator core network using IP via any suitable access technology.

5 Common requirements for Home NodeB / Home eNodeB

5.1 HNB and HeNB Installation, identification and location requirements

- H(e)NB shall have a unique equipment identity.

- All the H(e)NBs serving the same CSG share the same unique (within the PLMN) identity called CSG Identity.

NOTE: CSGs of different PLMNs are considered different, even if the PLMNs are indicated to the UE as "equivalent PLMNs" [10].

- It shall be possible to support at least 125 million CSG Identities within a PLMN of an operator.

- The radio transmitter of a H(e)NB shall not be activated until configured and authorised by the operator.

- When installing, provisioning, configuring or re-configuring an H(e)NB the operator shall be able to:

    - verify the H(e)NB's identity.

    - obtain the geographical location of the H(e)NB.

NOTE: The scenario where a H(e)NB is connected to one operator's network and later changed to another operator's network is not required.

- The operator shall be able to determine that the H(e)NB is installed and operated in accordance with all relevant regulatory requirements.

- The operator shall be able to configure the settings of the H(e)NB. In the case where the H(e)NB has detrimental impact on the spectrum usage, the H(e)NB can be set to out-of-service by the operator.

- Installation and activation of a new H(e)NB shall require no reconfiguration of the operator's network.

- The impact of H(e)NB on the core network should be minimised.

5.2   OA&M Requirements

- H(e)NB shall support the automatic discovery of an operator's management platform.

- It shall be possible to make use of the operator's management platform to carry out OA&M functions for H(e)NB. The management connection between H(e)NB and the operator's management platform shall be end-to-end secure.

- H(e)NB shall support OA&M procedures which allow the operator to remotely configure the H(e)NB, deploy software upgrades, detect and report changes in RF conditions and perform general OA&M tasks. The OA&M procedures shall be as closely aligned as possible with those that are commonly used in broadband access networks such as defined in TR-069 Amendment 2 [5].

- If the connection between H(e)NB and the rest of the operator network is out of service, then it shall be possible within an operator's defined time period for the H(e)NB to deactivate the air-interface.

- When the H(e)NB Hosting Party authentication is required by the MNO, the H(e)NB shall not activate the air-interface unless the authentication of the H(e)NB Hosting Party has been performed successfully.

5.3   Access Control requirements

5.3.1   General

- Subject to operator and H(e)NB Hosting Party agreement, the operator shall be able to configure the H(e)NB with open, hybrid or closed access mode.

- When the H(e)NB is configured for open access mode, it shall be possible for the H(e)NB to provide services to subscribers of any PLMN, subject to roaming agreement.

- When the H(e)NB is configured for hybrid access mode, it shall be possible for the H(e)NB to provide services to:

    - its associated CSG members, and

    - subscribers of any PLMN not belonging to its associated CSG, subject to roaming agreement.

- When the H(e)NB is configured for closed access mode, only users that belong to its associated CSG shall be able to obtain services.

- CSG members may include subscriber of any PLMN subject to roaming agreement, defined as HPLMN CSG Roaming.

- The VPLMN may support VPLMN Autonomous CSG Roaming by providing CSG membership to the roaming subscriber without exchanging any CSG specific information with the HPLMN. The VPLMN shall disable VPLMN Autonomous CSG Roaming on a per HPLMN basis if requested by the home operator.

NOTE: VPLMN Autonomous CSG Roaming and HPLMN CSG Roaming can be active in the same VPLMN

- The CSG membership granted to the subscriber during his stay in the VPLMN may be retained by the VPLMN (e.g. in case the subscriber moves to another PLMN and subsequently returns to the VPLMN).

5.3.2 Closed Subscriber Group

- The CSG manager shall be able, under the operator supervision, to add, remove and view CSG membership

NOTE: the interaction of the user with the application that manages the Allowed CSG Lists is out of scope of 3GPP (e.g. Web interface).

- For each subscriber, the network maintains a single CSG list containing the CSG identities that the subscriber is allowed to use.

- The UE shall contain a list of allowed CSG identities (Allowed CSG List). It shall be possible to store the Allowed CSG List in the USIM. When available, the list on the USIM shall be used. It shall be possible for both, the operator and the UE, to modify the Allowed CSG List.

- The UE shall allow the user to introduce new CSGs to the Allowed CSG List by means of manual CSG selection only.

- The UE shall maintain an operator-controlled list of allowed CSG identities (Operator CSG list). It shall be possible to store the Operator CSG list in the USIM. When available, the list on the USIM shall be used. It shall be possible for the operator to modify the Operator CSG List.

- The two lists are maintained independently from each other. A change in the Operator CSG list shall not trigger the UE to modify the Allowed CSG list to reflect such change automatically.

- Except during manual CSG selection, all CSG cells belonging to a CSG identity not included in the Allowed CSG List or Operator CSG list shall be considered not suitable by the UE ("not suitable" as specified in TS 25.304 [6] and TS 36.304 [7]).

- Each CSG identity shall be associated to a subscriber group which identifies the subscribers allowed to access the CSG.

- When the subscriber group is updated, the affected UE shall be informed accordingly.

- For temporary members, it shall be possible to limit the period of time during which the subscriber is considered a member of a CSG (granted access rights). It shall be possible to configure a time period for each temporary member.

- The time period shall be configurable by the CSG manager and/or the operator operating the CSG and shall span from 1 decihour to several days. Unlimited membership to the CSG is allowed.

- When a CSG is no longer considered available to provide services, except for emergency calls (i.e. due to time period expiry or removal of the CSG membership), it shall be possible to continue the established communication in another cell not belonging to this CSG.

- In hybrid access mode when services cannot be provided to a CSG member due to a shortage of H(e)NB resources it shall be possible to continue the established communication of non-CSG members in another cell.

- In hybrid access mode, to minimise the impact on CSG members from established communication of non-CSG members, it shall be possible for the network to allow the data rate of established PS communication of non-CSG members to be reduced.

5.4 Display requirements

5.4.1 CSG Type

The CSG Type is an indicator provided by the UE that is configured by the operator.

- It shall be possible for the operator to associate a CSG identity in the UE's Allowed CSG List or the Operator CSG List with a CSG Type. Therefore, it is possible that a CSG identity stored in different UEs may either be associated with the same CSG Type or with different CSG Types.

NOTE: The CSG Type allows, for example, information on the applied billing regime to be given to the user.

- When a UE camps on a cell with a CSG identity that is part of the UE's Allowed CSG List and or the Operator CSG List has an associated CSG Type, a UE that has a display capability shall provide the user with the associated CSG Type. A UE that does not have a display capability may provide the CSG Type by other means, e.g. voice notification.

- If the CSG Type for a CSG identity has not been configured in the UE, the UE may provide the HNB Name instead. In this case, the user is notified that the UE is providing the HNB Name rather than CSG Type.

- It shall be possible to store the CSG Type in the USIM. As an option, the CSG Type may be stored in the ME. If the CSG Type is present in the USIM, a CSG Type stored in the ME shall be ignored. If the CSG Type is present in the Operator CSG list, a CSG Type present in the Allowed CSG list shall be ignored.

- The CSG Type shall be stored in text and/or graphical format. When the CSG Type has a text component, the CSG Type text length shall not exceed 12 characters in any language.

5.4.2 HNB Name

HNB Name is a common name referring to HNB/HeNB as defined in TR 21.905 [1].

- It shall be possible for a CSG cell and for a hybrid cell to broadcast a HNB Name in free text format. The UE may display the HNB Name when camping on the cell where it is broadcasted. The HNB Name, if broadcasted or stored in the UE, shall be available to the user during manual CSG selection. The HNB Name shall be configurable by the operator or the H(e)NB Hosting Party at the discretion of the operator.

- The HNB Name length shall not exceed 48x8 bits.

NOTE 1: In order to allow the maximum flexibility in the way the HNB Name is configured in any language, UTF-8 coding should be used; this allows a maximum length of 48 characters coded on one byte, 24 characters on two bytes, 16 characters on 3 bytes down to a minimum of 12 characters if all characters are encoded on 4 bytes.

- If available and depending on operator preferences a HNB Name may be stored together with the associated CSG Identity in the UE's Operator CSG List.

- If available and depending on operator preferences a HNB Name may be stored together with the associated CSG Identity in the UE's Allowed CSG List.

- A HNB Name present in the Operator CSG list shall take precedence over a HNB Name present in the Allowed CSG list, which in turn shall take precedence over the broadcasted HNB Name.

NOTE 2: The UE's Operator CSG List and Allowed CSG List are stored on the USIM or, optionally, in the ME as specified in section 5.3.2.

NOTE 3: The HNB Name is necessary in order to aid the user in choosing the correct CSG identity when performing a manual CSG identity selection.

5.5 Mobility Aspects for Home NodeB and Home eNodeB

5.5.1 PLMN selection

The standard automatic and manual network selection procedures are used to register a UE on a PLMN via a H(e)NB.

5.5.2 Idle-mode operation

In addition to normal cell reselection procedures, the following requirements apply:

- It shall be possible to support idle mode mobility between a H(e)NB cell and other cells and between H(e)NB cells.

- A UE in idle mode shall prefer to select a cell whose CSG Identity is in the UE's Allowed CSG List or in the Operator CSG list, when the cell reselection criteria has been met.

    NOTE: All CSG identities on the Allowed CSG list and the Operator CSG list have the same priority.

- The cell reselection procedure should not result in excessive power consumption in the UE.

5.5.3 Connected mode operation

- It shall be possible to support service continuity, including handover, between a H(e)NB cell and other cells and between H(e)NB cells. This includes H(e)NB cells in residential and enterprise environment.

- For operational and deployment purposes, handovers between a H(e)NB cell and other cells and between H(e)NB cells should not significantly increase mobility related signalling.

- Data session(s) may be terminated by the network after the UE leaves the H(e)NB coverage area on a per UE basis (e.g. based on subscriber tariff change).

5.5.4 Manual CSG selection

The user shall be able to request the UE to perform a scan for available CSGs. When such request is received the UE shall perform a scan of available CSGs, their CSG Identities and their HNB Names. In the UE display, the available CSGs shall be represented by their associated HNB Names and PLMN Name(s). If the HNB Name is not available, the CSG Identity shall be displayed instead.

An indication shall be given to the user as to which of the available CSGs is contained in the Allowed CSG List or Operator CSG list. The available CSGs shall be displayed in the following order:

   - The CSGs, whose CSG Identities are contained in the Allowed CSG list.

   - The CSGs, whose CSG Identities are contained in the Operator CSG List.

   - Any other CSG, whose CSG Identity is not included in the Allowed CSG List or the Operator CSG list.

The HPLMN shall configure, on a PLMN basis, the UE to display the available CSGs so that either:

- all CSGs are displayed, or

- only CSGs in the Operator CSG List are displayed.

    NOTE: It is assumed that OMA DM/OTA will be used by the HPLMN to configure the ME/USIM

By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN, for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

When the user selects an entry in the list, the UE shall reselect any of the available cells with the CSG chosen by the user.

The UE shall attempt to register to the PLMN.

If the registration attempt is accepted, the UE shall add the CSG identity to the Allowed CSG list unless the cell is a hybrid cell or the identity is already present in the list.

If the registration attempt is accepted and the UE is allowed to add the CSG identity to the Allowed CSG list then the UE may add the broadcasted HNB Name to the Allowed CSG list.

If the registration attempt is rejected and the CSG entry is in the Allowed CSG list, that CSG and the associated HNB Name shall be removed from the Allowed CSG list.

In addition, when the user manually selects a CSG in a PLMN, which is different from the last registered PLMN, the following behaviour applies:

- The UE shall enter into Manual PLMN Selection state.

- The UE shall attempt to register to the PLMN. This PLMN shall not be stored as the Last Registered PLMN.

- When the UE is no longer in the service area of the CSG the UE shall return to the previous PLMN Selection state.

5.6 Services support

5.6.1 General

- Subject to availability of network resources there shall be no difference in the user experience when using the PLMN provided services via H(e)NB or via NodeB/eNodeB (NB/eNB).

- Depending on operator preferences and in compliance with regulatory requirements ETWS and PWS [9] shall be supported.

- Any additional registration and paging load as a result of H(e)NB deployment shall be minimized.

- Deployment of H(e)NBs and NB/eNBs on the same spectrum should not degrade the performance of UEs receiving service from NB/eNBs.

- Deployment of H(e)NBs and NB/eNBs on the same spectrum should not degrade the NB/eNB's coverage and capacity.

5.6.2 Emergency services

- Subject to local regulatory requirements, H(e)NB shall support emergency calls, as specified in TS 22.101 [4].

- It shall be possible for the operator to provide location information of the UE attempting an emergency call over a H(e)NB. The location information shall be sufficiently accurate to comply with the regulatory requirements that apply to the area where the H(e)NB is deployed.

5.6.3 IMS Interworking

- The operator can provide CS-to-IMS interworking as specified in the IMS Centralized Services clause of TS 22.101 [4].

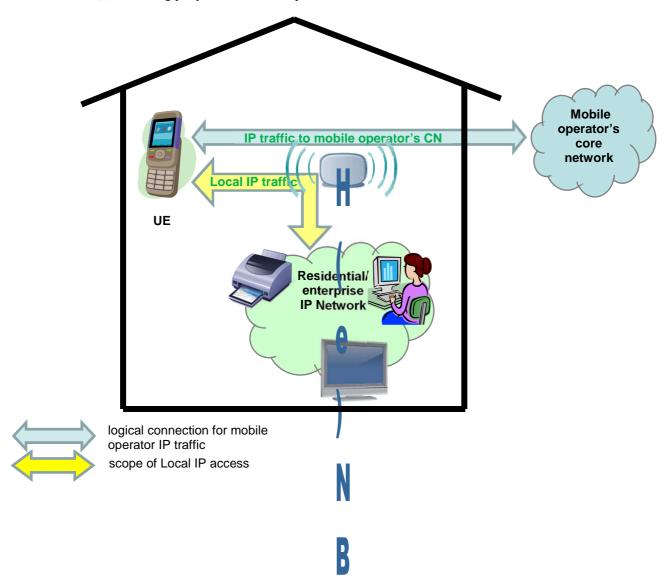# 5.7 Local IP Access (LIPA)

5.7.1 Description

Local IP Access provides access for IP capable UEs connected via a H(e)NB (i.e. using H(e)NB radio access) to other IP capable entities in the same residential/enterprise IP network. Data traffic for Local IP Access is expected to not traverse the mobile operator's network except mobile operator network components in the residential/enterprise

premises. Signaling traffic will continue to traverse the mobile operator network. The residential/enterprise IP network itself and the entities within that network are not within the scope of 3GPP standardisation.

NOTE: It is not precluded that a small amount of data traffic for Local IP Access (e.g. user packets that trigger paging) be forwarded via the mobile operator's network, provided there is a trust relationship between the H(e)NB hosting party and the mobile operator.

5.7.2   General requirements

A H(e)NB subsystem shall be able to support Local IP Access in order to provide access for IP capable UEs connected via a H(e)NB subsystem (i.e. using H(e)NB radio access) to other IP capable entities in the same residential/enterprise IP network.

-    Simultaneous access from a UE to the mobile operator's core network (e.g. internet, PLMN services) and Local IP Access to a residential/enterprise IP network shall be supported.

-    Subject to regulatory requirements, Local IP Access traffic shall be routable only between the UE, H(e)NB and other entities within the residential/enterprise IP network.

-    A UE shall have a valid subscription with the mobile operator in order to use Local IP Access.

- A UE shall be able to use Local IP Access in a visited network subject to roaming agreement between mobile operators.

- The HPLMN shall be able to enable/disable LIPA usage when the UE roams to particular VPLMNs.

- Local IP Access shall not affect services running in parallel for the same UE.

- Pre-Rel 10 UEs should be able to use Local IP Access.

- The user may be notified when a H(e)NB provides access to a residential/enterprise IP network

- A UE using Local IP Access shall be contactable by another IP endpoint in the same residential/enterprise IP network via Local IP Access.

- The operator shall be able to configure the network to support connection request from a UE so that a LIPA connection is used when the UE is located within the residential/enterprise IP network, and a regular connection via the Core Network is used otherwise.

- It shall be possible for a UE to maintain its IP connectivity to the residential/enterprise IP network when moving between H(e)NBs within the same residential/enterprise IP network. Any interruption to this IP connectivity shall be limited to levels comparable to that of the IP connectivity for PLMN services.

NOTE: Loss of access to the residential/enterprise IP network is acceptable as a UE moves out of H(e)NB coverage.

- The mobile operator shall be able to configure the H(e)NB to enable/disable Local IP Access.

- The mobile operator shall be able to enable/disable Local IP Access per user subscription per CSG.

- The H(e)NB Hosting Party, within the limits set by the mobile operator, shall be able enable/disable Local IP Access per H(e)NB.

- The H(e)NB subsystem shall allow the mobile operator to make traffic and signalling performance measurements related to Local IP Access for each user and for the H(e)NB.

- The H(e)NB subsystem shall allow the mobile operator to collect fault management information related to Local IP Access for each H(e)NB.

NOTE: It is possible for the H(e)NB Hosting Party to use additional access control mechanisms (e.g. using a password) to restrict access of UEs to the residential/corporate IP network. However, such additional access control is out of scope of 3GPP standardisation.

- Local IP Access shall not compromise the security of the mobile operator's network.

5.8 Managed Remote Access to home based network

- The H(e)NB may support remote access for a CSG member to the home based network from a UE via a PLMN in order to provide access to IP capable devices connected to the home based network.

- It shall be possible to restrict the access to the home based network on per-subscriber basis (e.g. some subscribers may have managed access to their home network and others may not).

5.9 Selected IP Traffic Offload (SIPTO) at Local Networks

It shall be possible that a H(e)NB SubSystem supports Selected IP Traffic Offload to provide access for a UE connected via a H(e)NB (i.e. using H(e)NB radio access) to a defined IP network (e.g. the Internet). The following requirements apply to the H(e)NB SubSystem to support Selected IP Traffic Offload at the local residential/enterprise IP network:

- Selected IP Traffic Offload shall be possible to be done without traversing the mobile operator network, subject to regulatory requirements.

- The mobile operator and the H(e)NB Hosting Party, within the limits set by the mobile operator, shall be able to enable/disable Selected IP Traffic Offload per H(e)NB.

- Based on mobile operator SIPTO policies and configured user consent per APN, the network shall be able to offload traffic.

Note: There is a possibility that the user's service experience will be different if the user's traffic is offloaded via SIPTO at local residential/enterprise IP networks.

- The SIPTO policies may be defined per APN or per IP flow:

    - SIPTO policies per APN indicate whether all traffic associated with a specific APN is subject to offload;

    - SIPTO policies per IP flow are routing policies indicating which APN to use for a specific IP flow. The Operator may provide routing policies to the UE that assist the UE in routing the IP flows towards an appropriate APN. This is applicable for UE regardless of whether or not it has established IP connectivity to the local enterprise/residential network.

- The mobile operator shall be able to configure the SIPTO policies either statically or dynamically.

- Simultaneous connectivity from the UE to the mobile operator's core network and to a defined IP network (e.g. the Internet) via a fixed residential/enterprise IP network using SIPTO shall be supported.

- Simultaneous access from the UE to PLMN services and to fixed services via a fixed residential/enterprise IP network using SIPTO shall be supported.

Requirements that are common with Selected IP Traffic Offload in the mobile operator networkcan be found in section 4.3.5 in [4].

5.10　UICC and H(e)NB

Optionally, the H(e)NB may support identification and authentication of the H(e)NB Hosting Party by means of a UICC-based application.

This application may also contain information for the initial provisioning (e.g. the O&M system contact).

If the H(e)NB supports the H(e)NB Hosting Party application,

- The H(e)NB shall support the use of the operator's UICC application management platform to configure the Hosting Party application.

- The UICC application shall be able to acquire the geographical location of the H(e)NB.

Note: UICC application management is specified in 3GPP TS 31.115 [11] and 3GPP TS 31.116 [12].

5.11　Void

5.11.1　Void

5.11.2　Void

6　Requirements for Home NodeB

6.1　Access Control

- It shall be possible to control access (i.e. accept and reject connection requests) of pre-Release 8 UEs.

NOTE:　Such mechanisms may be different for those used to access control a Release 8 UE.

- The operation of a HNB shall not adversely impact the performances of a pre-Release 8 UEs operating in the area where the HNB is active and vice versa.

- The total bandwidth from the HNB towards the network for 4 simultaneous TS11 or TS12, including signalling and overhead, shall not exceed 200 kbps

6.2 Void

7 Requirements for Home eNodeB

7.1 Services support

7.1.1 Void

8 Quality of Service

8.1 General

- Subject to agreement between the mobile operator and the broadband access provider, it shall be possible to request resources from the broadband IP backhaul for the QoS treatment for sessions traversing the H(e)NB subsystem.

8.2 Admission Control

- The network shall be able to perform admission control based on the available H(e)NB backhaul resource.

- The network shall be able to set different criteria for admissionThe network control in a hybrid cell for CSG and non-CSG members.

9 Security and privacy

9.1 General

- The use of H(e)NB shall not compromise the security of any PLMN or broadband access network.

9.2 Security Requirements

- The H(e)NB shall provide a high level of security, equivalent or better than Rel-8 3GPP systems.

- Security policy shall be under the control of the H(e)NB network operator.

- The H(e)NB shall not impact the security of the UE.

9.3 Privacy

- The H(e)NB shall not compromise user privacy for UEs that are using the H(e)NB, including communication confidentiality, location privacy and identity protection.

10 Charging Aspects

NOTE: Refer to charging requirements in TS 22.115 [8]

Annex A (informative): Use cases

These use cases do not imply any requirement beyond that which is contained in the normative part of this TS.

Usecase-1: H(e)NB Mobility

User A connects to the H(e)NB via mobile device. User A should be able to move around within the H(e)NB coverage in the home or enterprise. User should also be able to invoke additional services based on user policy and operator policy.

Usecase-2: H(e)NB Guest Users

User A and User B are subscribers of Operator 1 and Operator 2 respectively. User A visits User B in his home and User B allows User A to use H(e)NB in User B's home. User A should be able to access all the services he is subscribed to from Operator 1 based on the policies set by User B and operator 2. Operator 1 and Operator 2 have roaming agreement.

Usecase-3: HNB/HeNB – NB/eNB Handovers

User A subcribes to cellular services of Operator 1 and is authorised to access a HNB/HeNB from same or other operator. User A starts service in the H(e)NB coverage and continues moving into a cellular network. Similarly User A starts service in cellular network and continues moving into H(e)NB coverage. User A does not see any impact on services due to mobility in both cases.

Usecase-4: Access to Home based services

User A connects to the H(e)NB via mobile device. User A should be able to access home based services (e.g. local digital media servers and digital media players) from the mobile device. Other users may access the home based services subject to H(e)NB Hosting Party policies.

Usecase-5: Media Transfer

User A connects to the H(e)NB via mobile device. User A starts viewing video streaming service on the mobile device. User A then wants to continue viewing the video on a different screen for better viewing. User A should be able to transfer the session to a high-definition TV or PC connected via broadband connection. User A should also be able to transfer the session from the TV or PC to a mobile device and continue the session in the H(e)NB coverage and also in the cellular network.

Usecase-6: IMS capable <u>HNB used for coverage purposes</u>

In this scenario, the reason for an operator to introduce IMS capable HNB is to offload voice traffic from his existing CS core network to IMS. However, as in this scenario the usage of 'legacy' services (e.g. CS Fax) is still assumed - only the utilization of network resources is to be changed - it is requested that IMS capable HNB provides all the services/ capabilities that are provided through regular Node B from the beginning.

Usecase-7: IMS capable <u>HNB for a new business model</u>

This scenario starts with a view that HNB is located in the user's residence and the UE is the preferred equipment to interact with home services/ applications. New business can be expected there. In this scenario, some of the CS services/ capabilities that are provided through regular Node B might not be

needed or might be provided in a later step if the operator could instead offer attractive new services under IMS capable HNB only.

Usecase-8: IMS capable <u>HNB for Green field operator</u>

This scenario expects new players to get into the mobile market. In this scenario, they would aim to deploy cost efficient and future proof infrastructure, i.e. no CS domain but IMS/PS domain only, regardless of whether or not UEs have IMS client on them.

Usecase-9: Hybrid access mode

In order to improve the coverage in a shopping mall, H(e)NBs are deployed. The shopping mall owner may have been provided a special deal by the network operator where the employees of the shopping mall will get preferential charging rates and priority access when accessing services via these H(e)NBs. In exchange, the shopping mall owner allows the public to use the H(e)NBs to access the normal network operator services. The H(e)NB Hosting Party should not need to manage the public access and the public should not need to do anything special in order to get services on the H(e)NB.

Use case-10: Open access mode

Typically to enhance coverage or capacity of an operator's public network, for example in railway stations, airports, stadiums, etc, taking benefit of the H(e)NBs additional functionality (e.g. uncoordinated deployment).

Usecase-11: HNB interacts with Home network

User A connects with his UE (possibly a pre-Rel 9 UE) to the HNB with IMS Interworking and Local IP Access to the home network capabilities. The home network accommodates home network devices (Intercom, Door lock, Network radio, Photo server, etc.) and the HNB. User A should be able to communicate with a visitor at Intercom via the mobile device.

Usecase-12: HNB interacts with IP-PABX

User A connects with his UE (possibly a pre-Rel 9 UE) to a HNB with IMS Interworking and Local IP Access to the home network capabilities at an office. The HNB might be deployed and interconnect with an enterprise extension telephone system (e.g. SIP based PABX). User A should be able to make/receive an extension call to/from fixed line UE under SIP based PABX. In addition, User A with the mobile device and User B with computers should be able to access a common groupware server at the office and share the same information such as schedule, emails, etc.

Usecase-13: Electronic customer guide in shopping centre, using Local IP access

A department store or shopping centre provides electronic shopping guide. When user A enters into a shopping centre where a shopping centre H(e)NB is installed, an invitation indication shows up on his mobile device which he accepts. This allows him access to the centre's H(e)NB. Subsequently, he accesses the centre's customer service server, which is only accessible through the H(e)NB where he uploads his shopping list. The customer service server responds a list of sale items of similar nature. He accepts or declines the various choices and the final shopping list is downloaded to his UE. While user A is waiting, User A watches free TV show or advertisement provided through the H(e)NB for the shop customer. While in the shopping centre the user has simultaneous access to operator's and local shopping centre services.

Usecase-14: Local IP Access

The user has the subscription through home operator H. The user is served by the home operator H. The UE obtains IP connectivity in both a local gateway to obtain local connectivity for IMS services (e.g. as in local IP access or for enterprise scenarios with call to other terminals in the PABX area) and to a home gateway (as in normal connectivity for IMS services). For IMS sessions to be routed to e.g. remote terminals, the traffic is sent through the connectivity with the home gateway, whereas for IMS session that can be routed locally (e.g. based on local phone number), the traffic is sent through the connectivity with the local gateway through the local IP access. Whether the UE routes a specific IMS session through the local access or the home gateway can be controlled on a per session basis. Also, the UE may obtain local connectivity by default (e.g. based on static configuration by the operator) or dynamically based on indication by the IMS server.

Usecase-15:

Subscriber A from Network A owns HNB/HeNB A because of no macro network coverage .
Guest user B from Network B visits subscriber A's house. Subscriber A wants to allow guest user B access to HNB/HeNB A while the guest user B is visiting.

Usecase-16:

Corporation A has sites in country A, B and C.
Corporation A has employees from country A and B.
Employees in country A are from Operator AA and AB.
Employees in country B are from Operator B.
Corporation A has HNB/HeNB in country A from Operator AA and country B from Operator B.
Employees from country A and B are allowed access to HNB/HeNBs in country A and B.

Usecase-17: Content-sharing services in the residential IP network

During a trip to the zoo Alice has taken several pictures and has recorded a video clip on her UE. After returning home her UE connects to the H(e)NB in the home and accesses the residential IP network. The local devices (video, printer, ..) are automatically discovered by the UE. Alice views the videos on her video player, prints photos on her printer, uploads her media onto media server, and downloads media for her next outing.

Annex B (informative): Clarification of H(e)NB Access Modes

Table B.1 illustrates the different H(e)NB Access Modes and what access is allowed for UEs of any release depending on whether the UE is allowed access to the CSG.

In Table B.1 "Access" means "Access to services".

"Preferential access" means the user will get preferential access to the cell.

Table B.1: H(e)NB access for UEs of any release

	H(e)NB Access Mode		
	Open	Closed	Hybrid
UE allowed access to CSG	Access	Access	Preferential Access
UE not allowed access to CSG	Access	No Access	Access

NOTE: Pre Release 8 UEs can only access HNBs

Annex C (informative): Overview of identifiers and names.

Table C.1: Overview of identifiers and names

item	used for	associated with	permanently stored in	distribution method	displayed to user	comment
H(e)NB equipment identity	• administrative purposes	H(e)NB (physical entity)	• H(e)NB • administration database of the operator	O&M procedures	NO	not known to UE, therefore not useable by UE to identify a H(e)NB

CSG identity	• automatic and manual CSG selection
	• access control to CSG cells
		• a CSG, i.e. a group of users (UEs).
		• One or More H(e)NBs (CSG cells)
			• H(e)NB
			• administration database of the operator
			• Allowed CSG List in the UE if user (UE) is member of CSG (USIM entry takes precedence over ME)
				• provided by O&M to H(e)NBs
				• provided by home PLMN to UEs (the Home PLMN and Visited PLMN should synchronize this information)
				   o Provided to the UE by OMA DM when stored in the ME,
				   o Provided to the UE by OTA when stored in the USIM
				• Provided to UE via manual CSG selection
				• broadcasted by H(e)NB
					YES, if HNB Name is not available	A CSG identity is unique within a PLMN. In the UE a CSG ID, together with a network identifier, identifies a CSG globally uniquely.

HNB name (optional)	for supporting (ease of use) manual CSG selection, display-ing a "friendly" name to the user	CSG identity (relationship: m CSG ID : n HNB names)	• H(e)NB • administration database of the operator • UE	• Provided by O&M to H(e)NBs • Optionally stored by user in UE • broadcasted by H(e)NB	YES during manual selection, OPTIONAL during normal operation. (USIM entry takes precedence over broadcast and ME)	If a HNB name is stored in the UE it needs to be associated with a CSG identity. Initial configuration in the UE may be done by the operator (e.g. at point of sale). Later, a HNB name is implicitly associated to the current CSG identity by the UE when the user stores the HNB name
CSG Type	for additional information (on e.g. billing mode) to the user when camping on a CSG cell (i.e. after CSG has been selected)	CSG identity (relationship: n CSG ID : 1 CSG Type)	• administration database of the operator • UE	• provided by initial UE configuration, OTA and device management to UEs	YES, if CSG is in Allowed CSG List. (USIM entry takes precedence over ME)	UE needs to associate a CSG Type with a CSG identity Association done by operator (the Home PLMN and Visited PLMN should synchronize this information)

へ

Annex D (informative): Change history

TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	WI
SP-43	SP-090087	-	22.220	-	-	-	-	Approved by SA plenary.	2.0.0	9.0.0	EHNB
SP-44	SP-090373	S1-091273	22.220	0002	1	Rel-9	F	Clarification on the displaying of the H(e)NB name during manual CSG selection	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091164	22.220	0004	4	Rel-9	B	Optional USIM support in H(e)NB	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091387	22.220	0011	3	Rel-9	F	Clarification on Local IP Access Requirements	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091083	22.220	0015	-	Rel-9	F	Remove VPLMN CSG support for Rel9	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091382	22.220	0016	2	Rel-9	F	Clarification on the requirement of session diversion.	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091279	22.220	0019	2	Rel-9	F	Allowed CSG list management for hybrid cells	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091158	22.220	0023	3	Rel-9	D	Clarification of H(e)NB Owner / Hosting Party	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091159	22.220	0024	2	Rel-9	D	H(e)NB Operator Change	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091383	22.220	0025	2	Rel-9	F	Clarification of the terminology about H(e)NB access modes	9.0.0	9.1.0	EHNB
SP-44	SP-090373	S1-091274	22.220	0026	1	Rel-9	F	Minor corrections for clarification	9.0.0	9.1.0	EHNB
SP-44	SP-090374	S1-091260	22.220	0005	1	Rel-9	F	Rel 8 Rel 9 CSG lists alignment (approved at SA#44 but not implemented in 9.1.0)	9.1.0	9.1.1	EHNB
SP-45	SP-090477	S1-093332	22.220	0032	2	Rel-9	F	CSG Lists clarification	9.1.1	9.2.0	EHNB
SP-45	SP-090477	S1-093329	22.220	0035	1	Rel-9	F	IP access approach of backhaul network for H(e)NB	9.1.1	9.2.0	EHNB
SP-45	SP-090477	S1-093331	22.220	0037	1	Rel-9	D	Editorial corrections of TS 22.220	9.1.1	9.2.0	EHNB
SP-45	SP-090477	S1-093480	22.220	0039	2	Rel-9	C	Loss of IP Backhaul Connection	9.1.1	9.2.0	EHNB
SP-45	SP-090477	S1-093330	22.220	0041	1	Rel-9	F	Clarification of definition for H(e)NB Hosting Party	9.1.1	9.2.0	EHNB
SP-45	SP-090483	S1-093477	22.220	0038	4	Rel-10	F	CR to 22.220 on Clarification of QoS Requirements	9.1.1	10.0.0	TEI 10
SP-46	SP-090839	S1-094318	22.220	0057	1	Rel-10	A	Simplified CSG list handling	10.0.0	10.1.0	EHNB
SP-46	SP-090845	S1-094323	22.220	0067	2	Rel-10	B	H(e)NB mobility related load optimization	10.0.0	10.1.0	EHNBF
SP-46	SP-090845	S1-094380	22.220	0063	3	Rel-10	B	Requirements on HNBs in enterprise environments	10.0.0	10.1.0	EHNBF
SP-46	SP-090849	S1-094328	22.220	0046	3	Rel-10	B	Local IP Access requirements update	10.0.0	10.1.0	LIPA_S IPTO
SP-46	SP-090849	S1-094321	22.220	0047	2	Rel-10	B	Selected IP Traffic Offload Requirements for H(e)NB SubSystem	10.0.0	10.1.0	LIPA_S IPTO
SP-46	SP-090849	S1-094429	22.220	0062	1	Rel-10	B	Use case for digital content sharing with LIPA	10.0.0	10.1.0	EHNBF
SP-47	SP-100186	S1-100331	22.220	0072	1	Rel-10	B	Termination of data session	10.1.0	10.2.0	EHNBF
SP-47	SP-100186	S1-100328	22.220	0080	1	Rel-10	F	IMS HNB interworking alignment with SA2 decision	10.1.0	10.2.0	EHNBF
SP-47	SP-100186	S1-100453	22.220	0092	3	Rel-10	B	Add VPLMN CSG support for Rel-10	10.1.0	10.2.0	EHNB
SP-47	SP-100230	S1-100324r	22.220	0094	1	Rel-10	A	Clarification of the interaction of the Operator and Allowed CSG lists	10.1.0	10.2.0	EHNB
SP-47	SP-100187	S1-100316	22.220	0070	1	Rel-10	B	Mobility for Local IP Access (LIPA)	10.1.0	10.2.0	LIPA_S IPTO
SP-47	SP-100187	S1-100012	22.220	0071	-	Rel-10	F	Removal of SIPTO common requirements	10.1.0	10.2.0	LIPA_S IPTO
SP-47	SP-100187	S1-100326	22.220	0082	3	Rel-10	B	Clarification of requirements for LIPA	10.1.0	10.2.0	LIPA_S IPTO
SP-47	SP-100188	S1-100025	22.220	0073	-	Rel-10	A	H(e)NB Hosting Party USIM management	10.1.0	10.2.0	TEI-10
SP-48	SP-100402	S1-101248	22.220	0100	3	Rel-10	F	Enable/disable Selected IP Traffic Offload per H(e)NB	10.2.0	10.3.0	LIPA_S IPTO
SP-48	SP-100399	S1-101250	22.220	0101	4	Rel-10	F	Clarification of the CSG list in networks, Operator CSG list (OCL) and Allowed CSG list (ACL)	10.2.0	10.3.0	EHNBF

SP-49	SP-100573	S1-102388	22.220	0110	4	Rel-10	F	Removal of requirement to inhibit Allowed CSG List and VPLMN Autonomous CSG Roaming clarifications	10.3.0	10.4.0	EHNBF
SP-49	SP-100576	S1-102399	22.220	0106	3	Rel-10	F	Correction on HNB Name	10.3.0	10.4.0	EHNBF
SP-49	SP-100576	S1-102404	22.220	0107	4	Rel-10	F	Clarification of LIPA requirements	10.3.0	10.4.0	EHNBF
SP-49	SP-100578	S1-102197	22.220	0105	3	Rel-10	F	SIPTO for H(e)NB Subsystems Policy and User Interaction	10.3.0	10.4.0	LIPA_S IPTO
SP-49	SP-100578	S1-102400	22.220	0104	3	Rel-10	F	Enablement/disablement policies for LIPA	10.3.0	10.4.0	LIPA_S IPTO
SP-50	SP-100796	S1-103277	22.220	0117	1	Rel-10	F	Requirement on conditional LIPA	10.4.0	10.5.0	LIPA_S IPTO
SP-50	SP-100796	S1-103348	22.220	0118	3	Rel-10	F	Clarification on "enable/disable LIPA"	10.4.0	10.5.0	LIPA_S IPTO
SP-51	SP-110161	S1-110183	22.220	0123	2	Rel-11	A	Hosting Party Identity Module	11.0.0	11.1.0	TEI9
SP-51	SP-110172	S1-110178	22.220	0119	3	Rel-11	B	New Requirements for Enterprise Interworking scenario	11.0.0	11.1.0	TEI 11
SP-52	SP-110368	S1-111403	22.220	0133	1	Rel-11	A	Correction to the admission control for the H(e)NB	11.1.0	11.2.0	TEI11
SP-52	SP-110369	S1-111432	22.220	0129	1	Rel-11	A	Removal of PBX integration requirements	11.1.0	11.2.0	EHNBF
SP-52	SP-110376	S1-111126	22.220	0134	-	Rel-11	F	Clarification for SIPTO policy	11.1.0	11.2.0	TEI11
SP-53	SP-110582	S1-112387	22.220	0142	1	Rel-11	F	Clarification for SIPTO user consent	11.2.0	11.3.0	TEI11
SP-53	SP-110582	S1-112394	22.220	0136	1	Rel-11	F	SIPTO for the Local Residential/Enterprise Networks	11.2.0	11.3.0	TEI11
SP-53	SP-110582	S1-112395	22.220	0140	2	Rel-11	F	H(e)NB behaviour in case of absence of the UICC	11.2.0	11.3.0	TEI11
SP-53	SP-110582	S1-112396	22.220	0137	3	Rel-11	B	Allow the H(e)NB UICC application to acquire location Information	11.2.0	11.3.0	TEI11
SP-54	SP-110871	S1-113415r	22.220	0147	2	Rel-11	A	H(e)NB emergency call support	11.3.0	11.4.0	EHNB
SP-54	SP-110808	S1-113458	22.220	0149	1	Rel-11	A	MBMS not supported for HeNB	11.3.0	11.4.0	EHNB
SP-57	SP-120520	S1-122477	22.220	0156	3	Rel-11	A	Optional UICC authentication	11.5.0	11.6.0	TEI9
2014-10								Updated to Rel-12 by MCC	11.6.0	12.0.0	
2015-12	-	-	-	-	-	-	-	Updated to Rel-13 by MCC	12.0.0	13.0.0	
2017-03	-	-	-	-	-	-	-	Updated to Rel-14 by MCC	13.0.0	14.0.0	
2019-07	-	-	-	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	15.0.0	

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2020-07	SA#88e	-	-	-	-	Updated to Rel-16 by MCC	16.0.0

History

Document history		
V16.0.0	August 2020	Publication