3GPP TR 23.830 V9.0.0 (2009-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Architecture aspects of Home NodeB and Home eNodeB
(Release 9)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ^{TM}) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ^{TM} system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

3GPP, Architecture, Home NodeB, Home eNodeB

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword

This Technical Report 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

This Technical Report describes the architectural aspects of specific UTRAN and E-UTRAN base stations, known as Home NodeBs and Home eNodeBs, which provide services in e.g. residential or enterprise deployments.

NOTE: This feasibility study has led to normative modifications of various specifications; the contents of this technical report should therefore be considered out of date.

To achieve this, the objectives are to (a) document the architectural assumptions taken by other working groups as part of their previous and ongoing work on Home Node B/Home eNodeB and Closed Subscriber Groups (CSG), and to (b) identify any outstanding issues not properly addressed in Rel-8.

Starting from the resulting architectural baseline, the intention is to derive architectural requirements arising from the outstanding Rel-8 issues and the Rel-9 requirements on Home NodeB and Home eNodeB as laid down by SA WG1 in TS 22.220 [2]. Based on this, the objective is to discuss and conclude on solutions for the architectural issues arising from 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 22.220: "Service requirements for Home NodeBs and Home eNodeBs ".

[3] 3GPP TS 25.467: "UTRAN architecture for 3G Home NodeB; Stage 2".

[4] 3GPP TS 36.300: "E-UTRA and E-UTRAN; Overall description; Stage 2".

[5] 3GPP TS 36.331: "E-UTRA Radio Resource Control (RRC); Protocol specification".

[6] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[7] IETF RFC 4282: "The Network Access Identifier".

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].

Editor's Note: The following definitions are copied from TS 22.220 v1.0.0 and are intended to be used as baseline terminology for the work in SA WG2. As the work progresses these definitions may be revisited.

Closed access mode: HNB/HeNB operates as a CSG cell.

Closed Subscriber Group (CSG): A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells).

CSG cell: A cell, part of the PLMN, broadcasting a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. All the CSG cells sharing the same identity are identifiable as a single group for the purposes of mobility management and charging.

CSG identity: An identifier broadcast by a CSG cell or cells and used by the UE to facilitate access for authorised members of the associated Closed Subscriber Group. The scope and uniqueness of the CSG identity is within one PLMN, i.e. a certain value of a CSG identity may exist in more than one PLMN.

Allowed CSG list: A list stored in the network and the UE containing all the CSG identity information of the CSGs to which the subscriber belongs.

Home based network: An IP based network in the H(e)NB owner's premises that is connected to the H(e)NB.

Hybrid access mode: HNB/HeNB operates as a CSG cell where at the same time, non-CSG members are allowed access.

Open access mode: HNB/HeNB operates as a normal cell, i.e. non-CSG cell.

Editor's Note: The following definitions need to be reviewed:

CSG owner: A CSG owner is the owner of one or more H(e)NBs, that have been configured as a CSG cell(s) for a particular CSG. A CSG owner can, under the H(e)NB operator's supervision, add, remove and view the list of CSG members.

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 broadband IP backhaul.

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

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

H(e)NB Operator: A H(e)NB Operator is the PLMN operator under whose license a H(e)NB operates. A H(e)NB needs to be configured and authorised by the H(e)NB operator.

H(e)NB Owner: A H(e)NB Owner has a contractual relationship with the H(e)NB operator, related to running one or more H(e)NBs in the H(e)NB owner's premises.

NOTE: A H(e)NB Owner is likely to have the billing relationship with the H(e)NB operator. A H(e)NB Owner 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, optionally, the H(e)NB Gateway belonging to it.

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 Node B (over UTRAN)
HeNB:	Home Node B (over E-UTRAN)
HeMS:	Home(e)NodeB Management System
HNB GW:	Home Node B Gateway
SeGW:	Security Gateway

4 Architectural baseline and assumptions from Rel-8

Editor's Note: This section will provide an overview of the architectural work and architectural assumptions already made for Home NodeBs and Home eNodeBs by other working groups for Rel-8.

4.1 Impacting specifications/reports from other 3GPP WGs

Rel-8 work related to HeNB, HNB and CSG have been performed in a number of 3GPP working groups. The following list shows Rel-8 specifications and reports including HeNB, HNB and CSG:

SA WG1:

TS 22.011	Service accessibility.
TS 22.115	Service aspects; Charging and billing.

SA WG3:

TR 33.820	Security of H(e)NB.

RAN:

TS 36.300	Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2.
TS 36.413	Evolved Universal Terrestrial Radio Access (E-UTRA); S1 Application Protocol (S1AP).
TS 25.367	Mobility Procedures for Home Node B; Overall description; Stage 2.
TS 36.304	Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode.
TS 25.467	Technical Specification Group Radio Access Network (UTRAN); UTRAN Architecture for 3G HNB.
TS 25.468	Technical Specification Group Radio Access Network: UTRAN Iuh Interface RANAP User Adaption (RUA) signalling.
TS 25.469	Technical Specification Group Radio Access Network : UTRAN Iuh interface Home Node B Application Part (HNBAP).
TR R3.020	Home (e)NodeB; Network aspects.

CT WG1:

TS 23.122	Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
TS 24.008	Mobile radio interface Layer 3 specification; Core network protocols; Stage 3

TS 24.285	Allowed Closed Subscriber Group (CSG) List; Management Object (MO)
TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
TR 24.801	3GPP System Architecture Evolution (SAE); CT WG1 aspects

CT WG4:

TS 23.008	Organization of subscriber data
TS 23.003	Numbering, addressing and identification
TS 29.002	Mobile Application Part (MAP) specification
TS 29.272	MME Related Interfaces Based on Diameter Protocol

4.2 Home NodeB architectural baseline and assumptions

4.2.1 Architectural assumptions

- For pre-R8 UE, no new functions are added to the MSC/VLR, SGSN, HSS.
- For R8 UE, the essential functions (e.g. access control) are supported in the Core Network.
- HNB-GW performs NAS Node Selection Function (NNSF).
- The Allowed CSG List is part of the user's subscription data and stored in the HSS.

4.2.2 Architectural requirements

Editor's note: The relevant Home NodeB architecture requirements will be based on the service requirements in latest release 8 version of 22.011. Other architectural requirements may be derived from Rel 8 work in other groups.

Editor's note: Architectural requirements are expected to cover:

- distribution of functions on network nodes for Home NodeB support
- architecture support for discovery, security, authentication, and management processes related to Home NodeB
- HNB installation, identification and location requirements
- HNB backhaul efficiency
- Emergency service support

4.2.2.1 Support for CSGs and Allowed CSG List handling

- The Allowed CSG List shall be provided as part of the CSG subscriber's subscription data to the SGSN/MSC/VLR.

NOTE: The assumption for release 8 is the Allowed CSG List is stored in the HSS.

- When a CSG subscriber group is updated, the affected UEs' CSG subscription data shall be updated in the HSS. And then the HSS pushes updated subscription data to SGSN/MSC/VLR.
- The Allowed CSG List can be updated in the UE according to the result of attach, RAU/LAU, service request and detach procedures or by application level mechanisms such as OMA DM procedures.
- If a release 8 UE is rejected to access a CSG cell with the reject cause indicating it is not allowed to access a CSG cell, the UE shall remove the corresponding CSG ID from its locally stored Allowed CSG List.

- If a release 8 UE is accepted to access a CSG cell whose CSG ID is not included in the UE's locally stored Allowed CSG List, the UE shall add corresponding CSG ID into its locally stored Allowed CSG List.

4.2.2.2 Access control

- For pre-release 8 UEs, access control for HNB shall be performed in HNB GW and optionally in HNB.

- If the release 8 SGSN/MSC/VLR receives a NAS request message from the HNB GW together with an indication that the request is from a release 8 UE, the SGSN/MSC/VLR shall perform access control for HNB during corresponding attach, detach, service request, RAU and location update procedures.

Editor's note: Operators may choose to use the "pre-Release 8 access control" for Release 8 UEs.

Editor's note: Access control solution for HNB/HNB GW connected to pre-release8 core network is FFS.

- The Release 8 UE shall be notified of the cause of rejection by the network if it is not allowed to access a CSG cell.

NOTE: For pre-Release 8 UEs, proper existing rejection cause should be used to reject the UE if it is not allowed to access a CSG cell.

- When a CSG ID which is not included in the UE's Allowed CSG List is manually selected by the user, a RAU or location update procedure via the selected CSG cell shall be triggered immediately by the UE to allow the SGSN or MSC/VLR to perform CSG access control.

4.2.2.3 Mobility management

- The system shall allow flexibility on RAI/LAI assignment for CSG cells and non-CSG cells.

- The handover procedure from HNB to macro NodeB reuses the existing relocation procedure for macro NB.

- For idle UE mobility from HNB to Macro NB, the location area update procedure/routing area update procedure is reused if necessary.

- For Idle UE mobility from Macro NB to HNB, access control shall be performed within LAU/RAU procedure if it is initiated by the UE. This applies both to CSG capable UEs and non-CSG capable UEs.

4.2.3 Architecture model for Home NodeB access network

Editor's note: Possible additional functions and reference points are FFS.

4.2.3.1 Logical architecture

The Rel-8 baseline architecture is based on the Rel-8 RAN and CT architecture and assumptions.

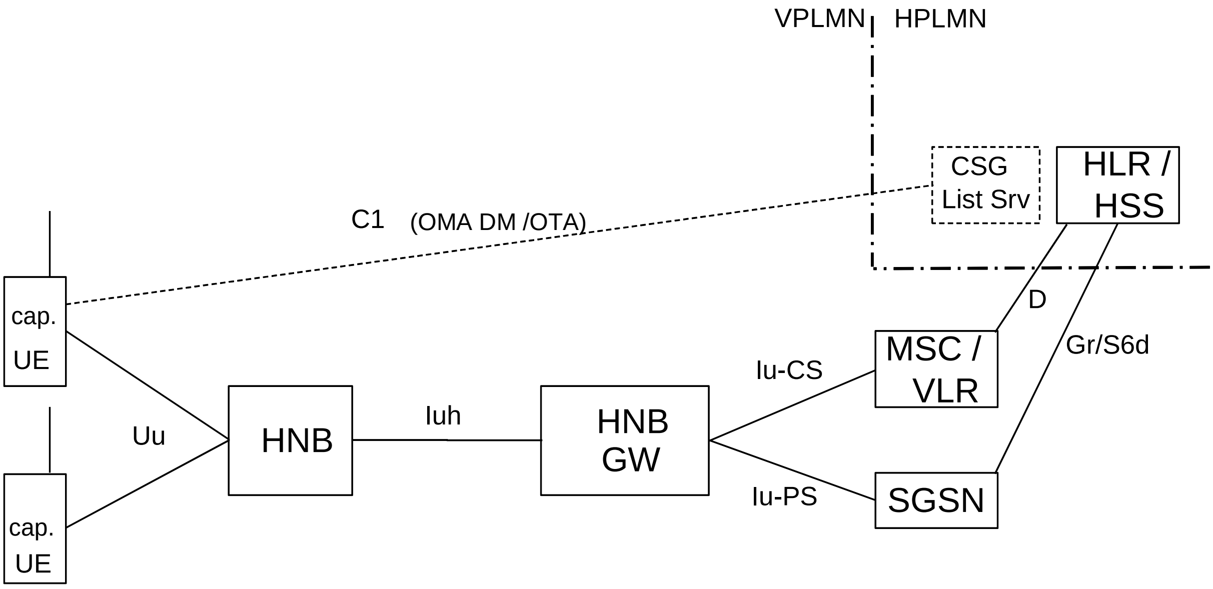

Figure 4.2.3.1-1: Logical architecture

NOTE 1:- Communication between the HNB and the HNB GW is secured by a mandatory Security Gateway (SeGW) function, which is not shown in the figure. The SeGW may be implemented either as a separate physical entity or integrated into the HNB GW.

NOTE 2 The optional C1 (OMA DM/OTA) interface may be used to update allowed CSG lists on CSG-capable UEs.

NOTE 3: It is FFS whether or not C1 is also applicable for temporary CSG members.

Editor's note: We have to decide whether the OAM nodes, OAM functions and associated reference points e.g. HMS (Home NodeB Management System) will be covered by this TR. Note that traditionally the OAM architecture is out of the scope of SA2 specifications.

4.2.3.2 Functional entities

HNB: The HNB provides the RAN connectivity using the Iuh interface, supports the NodeB and most of the RNC functions and also HNB authentication, HNB-GW discovery, HNB registration and UE registration over Iuh. The HNB secures the communication to/from the SeGW.

HNB GW: The HNB GW serves the purpose of a RNC presenting itself to the CN as a concentrator of HNB connections, i.e. the HNB-GW provides concentration function for the control plane and provides concentration function for the user plane. The HNB GW supports NAS Node Selection Function (NNSF).

SeGW: The Security Gateway is a mandatory logical function. It may be implemented either as a separate physical entity or integrated into the HNB-GW. The SeGW secures the communication from/to the HNB.

Editor's note: The security related functions of the HNB architecture are to be addressed by SA3.

CSG List Srv: The CSG List Server is an optional function allowing the network to update the allowed CSG lists on CSG-capable UEs.

4.2.3.3 Reference points

Uu: Standard Uu interface between the UE and the HNB.

Iuh: Interface between the HNB and HNB GW. For the control plane, Iuh uses HNBAP protocol to support HNB registration, UE registration and error handling functions. For the user plane, Iuh support user plane transport bearer handling.

Iu-CS: Standard Iu-CS interface between the HNB GW and the CS core network.

Iu-PS: Standard Iu-PS interface between the HNB GW and the PS core network.

D: Standard D interface between MSC/VLR and HLR/HSS.

Gr: Standard Gr interface between SGSN and HLR/HSS.

C1: Optional interface between the CSG List Srv and CSG-capable UEs. OTA is used to update the allowed CSG list on a UE with a Rel-8 USIM. OMA DM is used to update the Allowed CSG list on a UE with a pre-Rel-8 USIM.

4.2.3.4 Functional split

Editor's note: This section contains a table of high level HNB access function split between RAN and CN nodes.

Table 4.2.3.4-1: Home NB functional split

High-level Function	UICC	ME	HNB	HNB GW	SGSN	MSC/ VLR	HLR/ HSS	CSG List Server	Comments
HNB-GW Discovery			X						Determine the address of the Serving HNB-GW for a particular HNB.
HNB Registration			X	X					HNB reports its HNB identity, location information, operating parameters to HNB GW.
UE Registration for HNB			X	X					The UE Registration Function for HNB sets up the signalling context for the UE between HNB and HNB-GW and provides means for the HNB to convey UE identification data to the HNB-GW in order to perform access control for the UE in the HNB GW.
Access control (for non-CSG capable UE) (NOTE 1)			X	X					This function is used to decide whether a non-CSG capable UE can access a HNB cell. This procedure is part of the UE registration procedure. Access control is based on the UE's IMSI.
Access control (for CSG capable UE)					X	X			This function is used to decide whether a CSG capable UE can access a CSG cell.
Time period control (Editor's note 1)									Control the period of time during which (a temporary CSG user is allowed to camp on a CSG cell.
CSG membership management (Editor's note 2)									Add, remove and view the list of CSG members including the support of temporary CSG users
Allowed CSG List management (for CSG UE)	X	X					X	X	Management of the list of allowed CSG identities (per subscriber)
Manual CSG Selection	X	X			X	X	X		User manually selects a CSG. LAU/RAU shall be triggered after manual CSG selection to allow network perform CSG access control.
Idle Mode Mobility	X	X			X	X	X		Cell selection/reselection to/from CSG cell. This may trigger LAU/RAU.
Connected Mode mobility from HNB to Macro only (outbound)	X	X	X	X	X	X			Macro to macro mobility procedures (Non-CSG specific) are reused.
Paging optimization				X					A mechanism for filtering paging messages in order to avoid paging distribution to HNBs/CSG cells where

High-level Function	UICC	ME	HNB	HNB GW	SGSN	MSC/ VLR	HLR/ HSS	CSG List Server	Comments
									the UE is not registered
Emergency Services For non-CSG and CSG UE			X	X	X	X			Emergency calls for CSG and non-CSG members
NAS Node Selection Function				X					NNSF allows the support of Iu-Flex
Handling of connectionless SCCP messages			X	X	X	X			Connectionless SCCP messages sent by the HNB (e.g. Reset) need to be interworked to appropriate messages sent to the MSC/SGSN
Re-mapping of transport addresses				X					If the user plane goes through the HNB GW (e.g. for Iu over ATM), interception of control plane message and re-mapping of the user plane addresses (TEID and IP address).

NOTE 1: The support of this function in HNB is optional.

Editor's note: This function is still under consideration as an architectural issue for Release 8.

Editor's note: It is FFS whether the description of this function is in the scope of this TR. It is still under consideration as an architectural issue for Release 8.

4.3 Home eNodeB architectural baseline and assumptions

4.3.1 Architectural requirements

Editor's note: The relevant Home eNodeB architecture requirements will be based on the service requirements in latest release 8 version of TS 22.011. Other architectural requirements may be derived from Release 8 work in other groups.

Editor's note: Architectural requirements are expected to cover:

- distribution of functions on network nodes for Home eNodeB support.
- architecture support for discovery, security, authentication, and management processes related to Home eNodeB.
- architecture support for mobility and access control.
- Home eNodeB Installation, identification and location requirements.
- Home eNodeB backhaul efficiency.
- Emergency service support.

4.3.1.1 Support for CSGs and Allowed CSG List handling

- All Rel-8 onwards UEs supporting CSG functionality shall maintain a list of allowed CSG identities. This list can be empty in case the UE does not belong to any CSG.
- Each cell of a HeNB may belong to, at maximum, one CSG. It shall be possible for cells of a HeNB to belong to different CSGs and hence have different CSG IDs.

NOTE 1: The limitation of a cell of a HeNB belonging to only one CSG is due to limitation on the SIB-1 length, which allows for the name of only one CSG ID. See TS 36.331 [5].

- The Allowed CSG List shall be provided as part of the CSG subscriber's subscription data to the MME.

NOTE 2: The assumption for release 8 is the Allowed CSG List is stored in the HSS.

- When a CSG subscriber group is updated, the affected UEs' CSG subscription data shall be updated in the HSS. And then the HSS pushes updated subscription data to the MME.
- The Allowed CSG List can be updated in the UE according to the result of attach, TAU, service request and detach procedures or by application level mechanisms such as OMA DM procedures.
- If a release 8 UE is rejected to access a CSG cell with the reject cause indicating it is not allowed to access a CSG cell, the UE shall remove the corresponding CSG ID from its locally stored Allowed CSG List.
- If a release 8 UE is accepted to access a CSG cell whose CSG ID is not included in the UE's locally stored Allowed CSG List, the UE shall add corresponding CSG ID into its locally stored Allowed CSG List.

4.3.1.2 Access control

- The MME shall perform access control for the UEs accessing through CSG cells during attach, combined attach, detach, service request and TAU procedures.
- The UE shall be notified of the cause of rejection by the network if it is not allowed to access a CSG cell.
- When a CSG ID which is not included in the UE's Allowed CSG List is manually selected by the user, a TAU procedure via the selected CSG cell shall be triggered immediately by the UE to allow MME to perform CSG access control.

4.3.1.3 Mobility management

- There shall be no restriction on TAI assignment for E-UTRAN CSG cells, i.e.:
  - It shall be possible that a normal cell (non-CSG cell) and a CSG cell can share the same TAI or have different TAIs;
  - It shall be possible that CSG cells with different CSG ID can share the same TAI or have different TAIs;
  - It shall be possible that CSG cells with the same CSG ID can share the same TAI or have different TAIs.
- The concept of TAI list applies also for CSG cells. The TAI list may include TAIs related to CSG cells and TAIs related to non-CSG cells. The UE does not differentiate these TAIs in the TAI list.
- For the case of HeNB GW deployment, TAIs supported in the HeNB GW are the aggregation of TAIs supported by the CSG cells under this HeNB GW.

4.3.2 Architecture model for Home eNodeB access network

Editor's note: Possible additional functions and reference points are FFS.

4.3.2.1 Logical architecture

The Rel-8 baseline architecture variants are based on the Rel-8 RAN and CT architecture and assumptions.

4.3.2.1.1 Variant 1: With dedicated HeNB GW

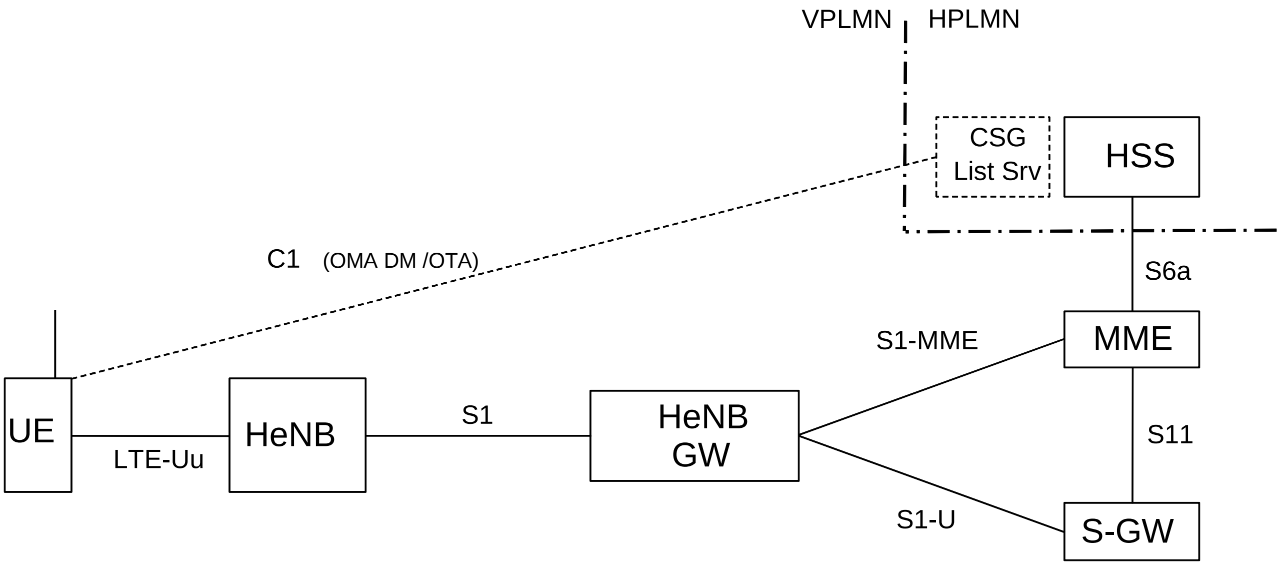

Figure 4.3.2.1.1-1: Variant 1: With dedicated HeNB GW

NOTE 1: Communication between the HeNB and the HeNB GW is secured by a mandatory Security Gateway (SeGW) function, which is not shown in the figure. The SeGW may be implemented either as a separate physical entity or integrated into the HeNB GW.

NOTE 2: The optional C1 (OMA DM/OTA) interface may be used to update allowed CSG lists on CSG-capable UEs.

Editor's note: We have to decide whether the OAM nodes, OAM functions and associated reference points e.g. HeMS (Home(e)NodeB Management System) will be covered by this TR. Note that traditionally the OAM architecture is out of the scope of SA2 specifications.

4.3.2.1.2 Variant 2: Without HeNB GW

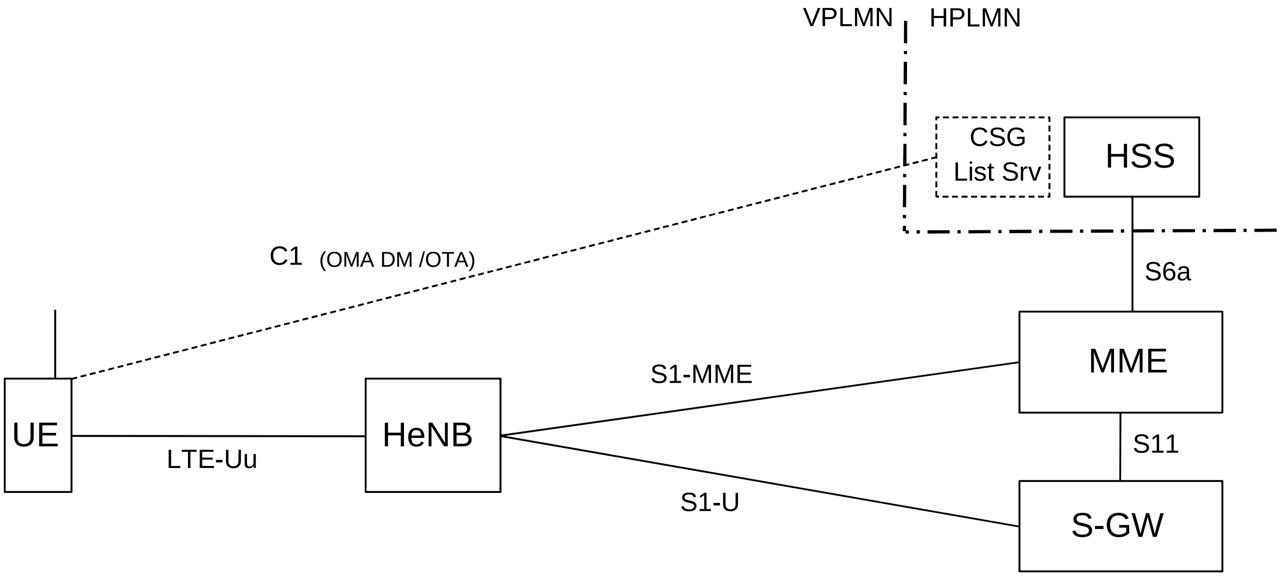

Figure 4.3.2.1.2-1: Variant 2: Without HeNB GW

NOTE: Communication between the HeNB and the MME/S-GW is secured by a mandatory Security Gateway (SeGW) function, which is not shown in the figure.

4.3.2.1.3 Variant 3: With HeNB GW for C-Plane

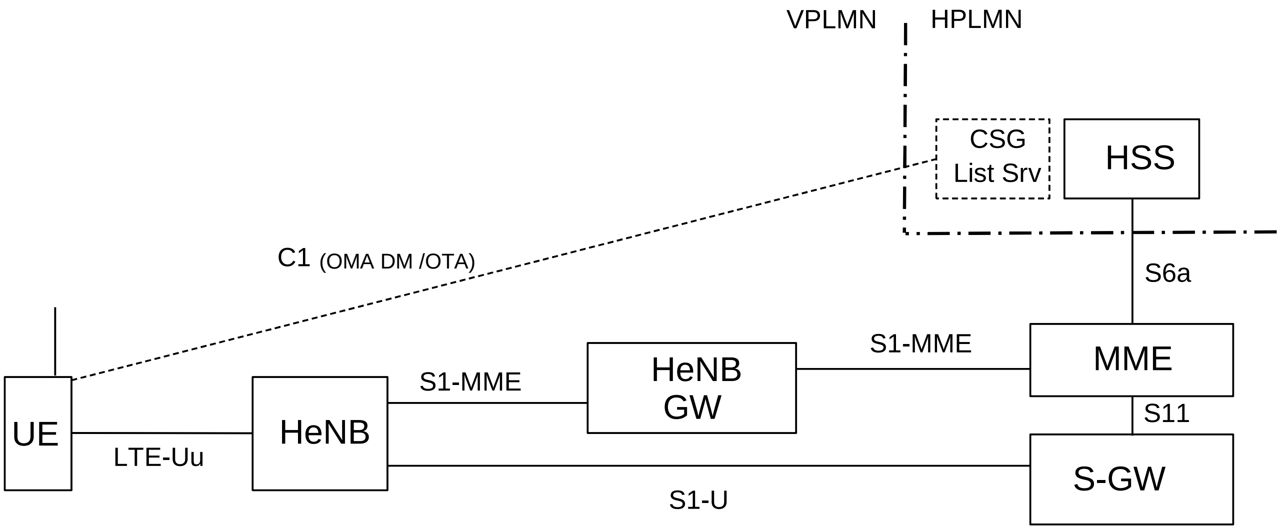

Figure 4.3.2.1.3-1: Variant 3: With HeNB GW for C-Plane

NOTE: Communication between the HeNB and the HeNB GW/S-GW is secured by a mandatory Security Gateway (SeGW) function, which is not shown in the figure.

4.3.2.2 Functional entities

HeNB: The functions supported by the HeNB shall be the same as those supported by an eNB (with the possible exception of NNSF) and the procedures run between a HeNB and the EPC shall be the same as those between an eNB and the EPC. The HeNB secures the communication to/from the SeGW.

HeNB GW: HeNB GW serves as a concentrator for the C-Plane, specifically the S1-MME interface. The HeNB GW may optionally terminate the user plane towards the HeNB and towards the S-GW, and provide a relay function for relaying User Plane data between the HeNB and the S-GW. The HeNB GW supports NAS Node Selection Function (NNSF).

SeGW: The Security Gateway is a mandatory logical function. It may be implemented either as a separate physical entity or co-located with an existing entity. The SeGW secures the communication from/to the HeNB.

Editor's note: The security related functions of the HeNB architecture are to be addressed by SA3.

CSG List Srv: The CSG List Server is an optional function allowing the network to update the allowed CSG lists on CSG-capable UEs.

4.3.2.3 Reference points

LTE-Uu: Standard LTE-Uu interface between the UE and the HeNB.

S1-MME: The S1-MME interface is defined between HeNB and MME if no HeNB GW is used. If HeNB GW is present, it shall use standard S1-MME interface towards both HeNB and MME.

S1-U: The S1-U data plane is defined between the HeNB, HeNB GW and the Serving Gateway. The S1-U interface from the HeNB may be terminated at the HeNB GW, or a direct logical U-Plane connection between HeNB and S-GW may be used.

S11: Standard interface between MME and Serving GW.

S6a: Standard interface between MME and HSS.

C1: Optional interface between the CSG List Srv and CSG-capable UEs. OTA is used to update the allowed CSG list on a UE with a Rel-8 USIM. OMA DM is used to update the Allowed CSG list on a UE with a pre-Rel-8 USIM.

There is no X2 interface between HeNBs and between eNB and HeNB.

4.3.2.4 High level functional split

Editor's note: This section contains a table of high level HNB access function split between RAN and CN nodes.

Table 4.3.2.4-1: Home eNB functional split

High-level Function	UICC	ME	HeNB	HeNB GW (NOTE 1)	MME	HLR/ HSS	CSG List Server	Comments
HeNB-GW Discovery			X					Determine the address of the Serving HeNB-GW for a particular HeNB.
Access control					X			This function is used to decide whether a UE can access a CSG cell.
S1-SETUP between HeNB and MME or HeNB GW			X	X	X			This procedure is used to establish S1 connection between HeNB and MME, or between HeNB and HeNB GW when HeNB GW is deployed.
Time period control (Editor's note 1)								Control the period of time during which a temporary CSG user is allowed to camp on a CSG cell
CSG membership management (Editor's note 2)								Add, remove and view the list of CSG members including the support of temporary CSG users
Allowed CSG List management	X	X				X	X	Management of the list of allowed CSG identities (per subscriber)
Manual CSG Selection	X	X			X	X		User manually selects a CSG. TAU shall be triggered after manual CSG selection to allow network perform CSG access control.
Idle Mode Mobility	X	X			X	X		Cell selection/reselection to/from CSG cell. This may trigger TAU.
Connected Mode mobility from HeNB to Macro only (Outbound)	X	X	X		X			Macro to macro mobility procedures (Non-CSG specific) are reused.
Paging optimization (NOTE 2)				X	X			A mechanism for filtering paging messages in order to avoid paging distribution to HeNBs/CSG cells where the UE is not registered
NAS Node Selection Function (NOTE 3)			X	X				NNSF allows the support of S1-Flex
Re-mapping of transport addresses				X				If the user plane goes through the HeNB GW, interception of control plane message and re-mapping of the user plane addresses (TEID and IP address).

NOTE 1: The presence of a HeNB GW is optional.
NOTE 2: Paging optimisation in MME and HeNB-GW are both optional.
NOTE 3: There is no S1 Flex function (NNSF) at the HeNB in case of connection to the HeNB GW.

Editor's note: This function is still under consideration as an architectural issue for Release 8.

Editor's note: It is FFS whether the description of this function is in the scope of this TR. It is still under consideration as an architectural issue for Release 8.

5 Architectural requirements

NOTE: the requirements below are in addition to the requirements already supported in Rel-8

5.1 General requirements

– Rel-9 core network. should be backward compatible with Rel-8 UE.

5.1.1 Installation, identification and location requirements

The following requirements are from TS 22.220:

- 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.
- It shall be possible to support at least 125 million CSG Identities within a PLMN of an operator.
- The impact of H(e)NB on the core network should be minimized.

5.1.2 CSG Membership Management

- In closed or hybrid mode, it should be possible for the CSG manager to add, remove and list the CSG members. It should be possible to add subscribers from another operator with which the HNB/HeNB operator has a roaming agreement.
- It shall be possible for the CSG manager and/or the operator operating the CSG cell to add/remove a roaming subscriber to a CSG without exchanging any CSG specific information with the HPLMN. In this case such CSG membership is acquired by the UE as a result of successful manual CSG selection.
- For temporary CSG members it shall be possible for the CSG manager and/or the operator operating the CSG cell to limit the period of time during which the subscriber is considered a member of a CSG (granted access rights).

5.1.3 Mobility management

5.1.3.1 Connected Mode

- Handover to or from an open H(e)NB shall be supported.

The requirements below apply to CSG cell in closed and hybrid mode:

- Handover from GERAN or UTRAN or E-UTRAN non-CSG cell to a UTRAN or E-UTRAN CSG cell shall be supported.
- Handover from UTRAN or E-UTRAN CSG cell to a UTRAN or E-UTRAN CSG cell shall be supported.
- Handover from UTRAN or E-UTRAN CSG cell to GERAN/UTRAN/E-UTRAN non-CSG cell shall be supported.

5.1.3.2 Idle Mode

- CSG Cell re-selection from UTRAN or E-UTRAN CSG cell to another UTRAN or E-UTRAN CSG cell shall be supported

5.1.4 Charging Requirements

The following requirements are related to HeNB from TS 22.115:

- It shall be possible to charge subscribers for consuming network services via a CSG cell based on the following information:
  - CSG identity of the CSG cell
  - subscriber membership of the CSG
  - type of service consumed by the subscriber
  - addition to and deletion from a CSG
- An operator shall be able to provide applicable tariffing information when a subscriber is added to a CSG.
- The network operator shall be able to charge both on-line and off-line for subscribers consuming network services via a HNB/HeNB CSG cell.

5.1.5 Emergency Services Requirements

The following requirements are from TS 22.220:

- H(e)NB shall support emergency calls for both CSG and non CSG members 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.

5.1.6 QoS and Admission Control Requirements

The following requirements are from TS 22.220:

- It shall be possible to provide information of the QoS treatment used for H(e)NB traffic traversing the H(e)NB to the H(e)NB broadband access mechanism.
- It shall be possible to perform admission control based on the available H(e)NB backhaul resource.
- It shall be possible for the network to set different criteria for access control in a CSG cell for CSG and non-CSG members.

5.1.7 Local IP Access in Home-based Network Requirements

The following requirements are from TS 22.220:

- It shall be possible that a H(e)NB supports Local IP Access to the home based network in order to provide access for a directly connected (i.e. using H(e)NB radio access), UE to other IP capable devices in the home. The following requirements apply to support Local IP access:
- Simultaneous access from a UE to both the operator's core network and Local IP Access to the home based network shall be supported.
- Access to local IP through the H(e)NB E-UTRAN/UTRAN-interface shall only be granted to UE with valid subscription.
- Pre-Rel-9 UEs should be able to use Local IP Access.
- It shall not be precluded for a device in the home based network to contact a UE via Local IP Access.

NOTE: Loss of access to Local IP Access is acceptable as a UE moves out of H(e)NB coverage.

- The operator or the H(e)NB Owner, within the limits set by the Operator, shall be able to enable/disable Local IP Access to the home based network per H(e)NB.
- It shall be possible to collect and make available to the operator statistics information (e.g. regular reporting of Local IP traffic volume) for each user on the use of the Local IP Access to the home based network.
- Local IP access to the home based network shall not compromise the security of the operator networks.

5.1.8 Local IP Access to Internet Requirements

The following requirements are from TS 22.220:

- It shall be possible to be done without traversing the operator network.
- Simultaneous access from a UE to both the operator's core network and Local IP Access to the Internet shall be supported.
- The operator or the H(e)NB Owner, within the limits set by the operator, shall be able to enable/disable Local IP Access to the Internet per H(e)NB.
- It shall be possible to collect and make available to the operator statistics information (e.g. regular reporting of Local IP traffic volume) for each user on the use of the Local IP Access to the Internet.
- Local IP access to the internet shall not compromise the security of the operator networks.

NOTE: When a UE is using the Local IP Access to the Internet, it is assumed that the H(e) NB does not provide any support to LI.

In addition, the following requirements shall be fulfilled:

- Local IP access to the Internet shall support the following two scenarios:
    - Scenario 1: H(e)NB and backhaul are provided by the same operator.
    - Scenario 2: H(e)NB and backhaul are provided by different operators.

5.1.9 Managed Remote Access to home based network

The following requirements are from TS 22.220:

- 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).

5.2 Home NodeB specific requirements

5.2.1 Access control

- Rel-8 SGSN/MSC stores the UE's Allowed CSG list and uses it to perform UE access control if the CSG ID and access mode of the Home NodeB are forwarded by the Home NodeB GW.
- Home NodeB GW performs UE access control if the UE is not CSG capable or if the SGSN/MSC is pre-Rel-8.

5.3 Home eNodeB specific requirements

5.3.1 General requirements

- Impacts to core-network interfaces to HeNB subsystem (S1-U and S1-MME) will be minimized.

5.3.2 Access control

- MME stores the UE's allowed CSG list to perform UE access control.
- CSG Id and access mode of the Home eNodeB shall be informed to the MME by the Home eNodeB for UE access control.

5.3.3 Mobility management

Editor's note: It is FFS whether there is any specific requirement in addition to 5.1.2.

6 Architectural issues and solutions

Editor's note: This section will discuss solution alternatives for architectural issues arising from (a) the service requirements for Home NodeBs and Home eNodeBs as laid down by SA1 and (b) requirements listed in clause 5 of this document.

The section is subdivided into releases that architectural issues apply to. Each architectural issue is structured as follows:

6.x.y Architectural Issue – ABC

6.x.y.1 Description

6.x.y.2. Solutions

6.x.y.2.1 Solution 1

6.x.y.2.2 Solution 2

6.x.y.3. Evaluation

6.1 Release 8

6.1.1 void

6.1.2 Architectural issue - Needs for a master list of CSG IDs in VPLMN

6.1.2.1 Description

To enable the H(e)NB owner to view the list of CSG members can be implemented according to two different principles (it is FFS if any additional alternatives exists) and also questions the overall requirement. It is assumed that one or more intermediate entities exist, and they are here called node A for simplicity:

Alt 1: The HeNB owner contacts node A each time a CSG member is added or removed. Node A contacts the HSS of the CSG members to add or remove the CSG Id. Node A stores a list containing necessary information for how to reach each CSG members HSS. If the H(e)NB owner wants to view the list of CSG members, the Node A can query each HSS in the list to retrieve CSG Id data.

Alt 2: The HeNB owner contacts node A each time a CSG member is added or removed. Node A contacts the HSS of the CSG members to add or remove the CSG Id, and Node A in addition stores the complete list of subscribers for this CSG Id. If the H(e)NB owner wants to view the list of CSG members, Node A can provide this information locally.

Alt 3: Is there a need for review by HNB owner, then no intermediate storage needed. Also the HNB might keep the list.

6.1.2.2 Solutions

6.1.2.2.1 Solution 1

In this clause it is proposed that the procedure for viewing of permanent CSG members is different from the procedure for viewing of temporary members.

For the permanent CSG members it is FFS whether the members could be added on-the-fly. Given that any addition/deletion of a permanent CSG member requires changes to the subscriber's profile in the HSS and in some cases it requires inter-PLMN information exchange, it may be so that the permanent members are best managed via formal communication in writing. For example, the following steps may be necessary for addition of a new permanent CSG member:

- the H(e)NB owner makes a written request to his PLMN ("PLMN A") for addition of a visiting friend ("Subscriber B");
- PLMN A then engages in a formal procedure with its roaming partner ("PLMN B") who owns the subscription of Subscriber B;
- after having received the consent from Subscriber B, PLMN B eventually updates the Subscriber B's profile in the HSS of PLMN B;
- following which PLMN A may also update the "H(e)NB Data Base" record of the H(e)NB owner by adding the Subscriber B's identity as a new permanent CSG member.

The "H(e)NB Data Base" record containing the permanent CSG members for a specific CSG ID is stored in a H(e)NB Data Base owned by the PLMN operator who operates the CSG. The Home(e)NB Data Base need not be collocated with the HSS that stores the subscription profile of the H(e)NB owner.

The H(e)NB owner should be able to query the H(e)NB Data Base at any time via a web-based interface that is outside of the 3GPP standardisation scope.

Regarding temporary CSG members, this clause assumes that temporary CSG membership is handled at the network periphery as described in clause in 6.1.1.2.1. The "Temporary CSG Member list" is stored in the local CN node (i.e. MME, MSC or SGSN) and the Access Provisioning Server in the H(e)NB is involved in every dynamic membership update. Because of this, the list of temporary CSG ID members can be stored locally at the H(e)NB and can be viewed by making a local query to the Access Provisioning Server in the H(e)NB.

NOTE: In this solution there is no need for 3GPP standardisation of the interface and/or the procedures used for viewing of either permanent or temporary CSG members.

6.1.2.3 Evaluation

6.1.3 Architectural issue - Identity used for CSG members (Rel-8?)

6.1.3.1 Description

What identity shall the CSG manager use to identify mobile subscribers when adding, removing or viewing the CSG members?

The CSG Manager uses these identities to complete administrative interaction with the H(e)NB operator. These interactions will result in some form of O&M procedure by the operator to either add or remove or view CSG membership to the identified subscribers. This issue does not concern identities that will be used by the core or radio access network.

Criteria for mobile subscriber identities for use by CSG Managers to communicate with H(e)NB Operators:

- comprehensible and easily produced by the CSG manager, who we cannot assume has the skills of a network administrator.
- recognizable and unambiguous to a mobile operator.
- a value a mobile subscriber knows, or could know.
- sufficient to identify not only the subscriber but also the subscriber's mobile operator.

Alternative identities:

- Alt A: IMSI is the most common identifier in the CN, but it can be questioned if it shall be used from a confidentiality perspective.

- Alt B: Another alternative is the MSISDN, which is well-known to each subscriber. It probably requires a one to one mapping between IMSI and MSISDN, which may not always be the case in all PLMNs.

- Alt C: The Network Access Identifier (NAI) [RFC4282] could be used to represent the user and home operator in an unambiguous fashion. An NAI has the syntax of an email address, meaning it can be easily remembered, spoken and entered using a keyboard by a third party. The NAI, if granted by the subscriber's home operator, would be unambiguous and identify also the HPLMN.

- Alt D: The UICC card associated with a subscription includes a serial number that can be used to identify the subscription. The UICC card also generally identifies the operator who issued it.

6.1.3.2 Solutions

6.1.3.2.1 Solution 1

It is left to the discretion of the H(e)NB operator which of the four alternatives should be used. All four of the alternatives would suffice to satisfy the four criteria.

Table 6.1.3.2.1-1: Solution 1

Alternative	How to determine the identity	How these meet the criteria
A) IMSI	Currently it is not apparent to a subscriber what the IMSI associated with their subscription is. A new "*#" code could be standardized for MMI to enable a subscriber to directly query their device.	- An IMSI is a serial number and therefore would be relatively straightforward for a H(e)NB owner to convey to the H(e)NB operator. - An IMSI unambiguously corresponds to a subscriber. - Currently an IMSI is not a value a subscriber knows, an additional mechanism would be needed to reveal it. - It is possible to infer the network operator from the IMSI
B) MSISDN	A subscriber will know their phone number or (for other devices such as data cards) can determine this assigned number as it is often assigned and could be included in owner documentation.	- A MSISDN is easily comprehended and conveyed. - An MSIDN may be used by several subscriptions, in a multi-SIM device, but in most cases there is a direct correspondence between a MSISDN and a subscription. - An MSISDN is a value that a subscriber knows or could determine. - It is possible to determine which operator an MSISDN corresponds to, but in most cases this is both possible and relatively straightforward. For example, the Enum standard, RFC 3761 [6], allows an MSISDN to be resolved to a particular URI by means of DNS. This could be leveraged to determine the operator.
C) NAI	A subscriber could be assigned an NAI value, and in many cases the subscriber already has such a value assigned (an email address, for example.)	- An NAI is easily comprehended and conveyed. - An NAI, if assigned, could unambiguously identify a subscription and is currently used for this purpose (see RFC 4282 [7]). - An NAI is a value that the subscriber knows or could know. - It is possible to determine which operator an NAI corresponds to. The 'realm' portion of the NAI identifies the operator (see RFC 4282 [7]).
D) UICC serial number + some operator identification	Examination of the UICC itself, for example inside a mobile device or consumer appliance.	- A serial number and operator identification is easily comprehended and conveyed. - The UICC serial number will uniquely identify a subscriber. - If the UICC is physically accessible, the UICC serial number should be easy to determine. - It should be possible to identify the operator from the exterior of the UICC (e.g. branding information identifying the operator).

6.1.3.3 Evaluation

An operator may choose one or more of the four alternatives outlined in Solution 1. Each of these satisfies the criteria, though some considerations are noted below. Taken together, these four alternatives satisfy the issue

Some considerations are worth noting regarding each of the alternatives.

(A) IMSI

The IMSI is not currently known to subscribers, a new mechanism to convey it would be required.

Use of the IMSI by H(e)NB owners for administrative procedures could present unacceptable security and confidentiality concerns. Use of the IMSI for identification of subscribers *outside of signalling* would require further analysis by SA3.

(B) MSISDN

In some cases there may be no MSISDN assigned (e.g. some SIP phones).

A single MSISDN could be assigned to multiple subscriptions (e.g. a multi-SIM device).

(C) NAI

Currently many subscribers do not have an NAI assigned to them.

(D) UICC serial number and operator identification

It may be difficult to physically access the UICC card.

The UICC card would have to include some form of operator identification (e.g. branding information) in order to meet the criteria.

Additional considerations apply to the process by which the CSG manager interacts with the H(e)NB operator:

A CSG Manager can only successfully add members who are subscribers of operators who have roaming agreements with the H(e)NB Owner's operator. This effectively restricts the range of potential H(e)NB Guests Users; some users cannot obtain guest access to some H(e)NBs. For this reason, some identities corresponding to mobile subscribers (that is, for potential invited guests) may not be understood by all H(e)NB Operators.

The identity used for the guest user needs to be translated into an IMSI, either by the H(e)NB Operator or by another operator with whom the H(e)NB Operator has a roaming agreement. This translation must occur before the CSG ID chosen by the CSG manager may be added to the guest user's subscription in the guest user's operator's HSS. Some types of identity may not be easily translated into an IMSI by the H(e)NB operator or other operators with whom the H(e)NB operator has a roaming agreement. Therefore, successful identification of subscribers by the CSG manager may require more than one type of identity be supported for interaction between operators or even for a given operator.

6.1.4 Architectural issue - Managing changes to CSG membership and handling of CSG ID expiration time

6.1.4.1 Description

The handling of the CSG ID expiration timer need to be defined, regarding what functions that are to be performed in which nodes. In addition it is needed to find a solution on how the synchronization is achieved between the UE and the MME/SGSN/MSC, to avoid that the UE is camping on a CSG cell that the MME/SGSN/MSC regards as not allowed for the UE. If the synchronization fails, it will lead to that the UE cannot be reached by a page, since it is camping on a CSG cell that MME/SGSN/MSC regards as not allowed for this UE.

Synchronization between UE and MME/SGSN/MSC is also needed in the case where a CSG ID is removed from the HSS, or the expiration time is changed in HSS. The assumption is that a solution covering the case of changed CSG data in HSS also can be used for synchronization when a CSG ID timer expires.

6.1.4.2 Solutions

6.1.4.2.1 Solution 1

Since the expiration date for a CSG ID exists in HSS and MME/SGSN/MSC, it seems needed that all entities handle the expiration date in some way.

Functionality in HSS:

- The HSS must supervise the expiration dates of any CSG ID in the subscription data, to be able to only send valid CSG IDs with corresponding expiration dates (i.e. not expired ones) in subscription data to MME/SGSN/MSC (e.g. in the existing Insert Subscriber Data message to SGSN). Otherwise the result would be that the CSG list in HSS might grow over time, not allowing new CSG IDs to be entered due to the maximum limit of 50 CSG IDs per subscriber.

- When a CSG ID expires, it implies that subscription data in HSS is changed. It is proposed that HSS shall not inform MME/SGSN/MSC each time any CSG ID for any subscriber expires. Another option is to let HSS supervise the timers, and to update MME/SGSN/MSC each time a timer expires, but this seems to increase the signalling from HSS to MME/SGSN/MSC and is therefore not preferred.
- If a new CSG ID is added or removed in the subscribers CSG ID list in HSS, or an expiration time is changed, it seems necessary to always send the complete list of CSG IDs to MME/SGSN/MSC according to current CT WG4 specifications.

Functionality in MME/SGSN/MSC:

- It is assumed that MME, SGSN and MSC have the same type of functionality for timer expiration handling.
- At any type of access control of a UE entering a CSG cell, the MME/SGSN/MSC must check that the CSG ID of the CSG cell corresponds to a CSG ID in the subscription data, and in addition that the expiration date hasn't passed.
- If the MME/SGSN/MSC receives updated subscription data from HSS, it needs to check whether any CGS ID is removed, or any expiration time is changed. No action is required if one or several CSG ID are added.
- If the expiration time for a CSG ID for an attached user expires, it seems needed that MME/SGSN/MSC performs the following actions:
  - If the UE is in Idle mode, MME/SGSN/MSC pages the UE.

Editor's note: Paging UE in Idle mode needed or not is for further study.

  - There are three possible cases:
    - The UE is camped on the CSG ID that has expired. Solution: The page will lead to the UE performing a Service Request. This Service Request can then be rejected by the MME/SGSN/MSC with an appropriate cause code, indicating that the CSG ID is not allowed. The UE will then remove this CSG ID from its list of Allowed CSG IDs, and will move into macro coverage, or into another CSG cell, depending on the content of its Allowed CSG ID list.
    - The UE is camped on another cell than the CSG cell with the CSG ID that has expired. Solution: The MME/SGSN/MSC accepts the Service Request and informs the UE of the expired CSG ID. It is FFS what mechanism to use to inform the UE of the expired CSG ID.
    - The UE is not reachable. Solution: The MME/SGSN/MSC do not remove the expired CSG ID, but marks it for removal. If there are incoming data for the UE, it will be also paged in cells of these CSD IDs. The CSG ID is not removed until the MME/SGSN/MSC can reach the UE and confirm that the UE has updated its list. It is FFS how to handle the case when the UE attaches to another MME/SGSN/MSC when it becomes reachable again.
  - If the UE is in Connected mode, there are two possible cases:
    - The UE is connected via the CSG cell of the expired CSG ID. Solution: MME/SGSN/MSC performs an S1-release or Iu-release with an appropriate cause code. This shall lead to the UE performing a TAU/RAU/LAU in macro-cell (or another CSG cell) and removing the expired CSG ID from its list of Allowed CSG IDs.
    - The UE is connected via another cell than the CSG cell of the expired CSG ID. Solution: It is FFS how the UE is notified of the expiry of the CSG ID.
  - Note that the requirement for Rel-9 is to divert the traffic to a non-CSG cell, which may require new procedures for network initiated handovers.

Disadvantages of placing the functionality in the UE:

- It can be discussed whether the UE in addition also need to know the expiration time. However, it does not seem possible to trust the UE to always obey the expiration time, which means that MME/SGSN/MSC must supervise it anyway. Therefore it would be duplicate functionality to require the UE to also supervise the expiration time.

- The UE does not get the expiration time according to existing standardisation work in other bodies, and it is neither required by SA1. One way to get the expiration time to the UE is to send it from the OMA DM server in addition to the CSG IDs, but this do not cover the cases where operators do not use OMA DM servers and rely on manual CSG ID addition. So in such cases would MME/SGSN/MSC anyway need to supervise the expiration time, or to add new procedures to convey the expiration time to the UE

- The expiration time for a CSG ID is defined by CT4 to be an absolute time. For a UE it doesn't seem trivial to precisely supervise that an absolute time has expired, and in such cases would the MME/SGSN/MSC anyway need to supervise it. An alternative is to add procedures to let the network convey absolute time to the UE, but this will introduce additional complexity in the UE and the network.

- Since it is concluded above that MME/SGSN/MSC must supervise the expiration time, an expiration time in the UE as well seems to cause race conditions and unnecessary signalling, since both the MME/SGSN/MSC and the UE at probably the same time tries to perform similar actions at CSG ID expiration.

- Due to the above reasons it is proposed that the UE do not receive or handle the expiration time for a CSG ID.

Functionality in other entities:

- It is also possible for a potential CSG list server to inform the UE over OMA DM of a changed list of allowed CSG IDs, caused by the expiration time for a CSG ID.

6.1.4.3 Evaluation

The following functionality is agreed for handling CSG membership changes for permanent and temporary CSG members.

Current functionality defined for HSS:

- The HSS sends the CSG subscription data including any potential expiration time to the MME/SGSN/MSC.

- If a CSG Id is added or removed in the CSG subscription data in the HSS, or an expiration time is changed, then the HSS shall send the update to the MME/SGSN/MSC.

Proposed additional functionality in HSS to handle changes in CSG membership:

- If a CSG Id is to be removed from the CSG subscription data, or the CSG ID is expired, then the HSS should remove the CSG ID from the HSS subscription data after the CSG ID was removed from the UE list, e.g. by OMA DM or OTA update, FFS how to accomplish when OMA DM or OTA are not deployed.

NOTE 1: It is FFS whether the other mechanisms besides OMA DM or OTA are needed to reduce the amount of time a UE will be out of service at a CSG cell when the subscriber has been removed from the CSG or the timer has expired.

- The HSS shall not update the CSG subscription data in MME/SGSN/MSC because of expiry of a CSG Id.

NOTE 2: This is just to reduce the amount of communication between the HSS and the MME/SGSN/MSC and it is functionally not needed.

- When the HSS stores CSG IDs with an expired time, these shall also be included in the CSG subscription data sent to the MME/SGSN/MSC.

- If a network uses paging optimisation Permanent CSG subscriptions should get an appropriate expiration time in HSS when the CSG subscription is cancelled. Subscription data in MME/SGSN/MSC are updated by the HSS because of this change of the HSS CSG subscription data.

NOTE 3: Using the expiry time information in the CSG subscriber data makes it possible to ensure that the MME that uses paging optimisation can page UEs that still may camp on that CSG when the subscriber has been removed from the CSG or the timer has expired. The CSG expiry time set to an expired value will indicate that the UE has not updated its Allowed CSG list when the UE was removed from a CSG or the CSG has expired for a temporary membership.

Current functionality defined for MME/SGSN/MSC:

- The MME, SGSN and MSC shall supervise the expiration time of any CSG Id in the subscription data, i.e., even if the UE knows the expiration time, the MME, SGSN and MSC shall not rely on the UE's enforcement of the expiration time for the CSG.
- When a UE accesses a CSG cell, the MME/SGSN/MSC shall check that the CSG Id of the CSG cell corresponds to a CSG Id in the CSG subscription data, and that the expiration time (if present) is still valid.
- In the event the UE accesses a closed CSG cell either due to being paged at the CSG, initiating uplink data transfer, initiating a mobile originating call or initiating a LAU/RAU/TAU procedure (e.g. triggered by an automatic or manual reselection), if the CSG Id is not present in the CSG subscription data or the timer has expired, then the MME/SGSN/MSC shall send a reject message with the appropriate error code. The UE shall remove the entry for this CSG from the Allowed CSG list.

NOTE 4: It is FFS whether the reject message with the appropriate error code needs to be integrity protected

Proposed functionality in MME/SGSN/MSC to handle changes in CSG membership:

- When a CSG subscription has expired, the entry for this CSG in the Allowed CSG list of the UE may not yet have been removed, and the UE may be camped on a CSG cell for that CSG in idle mode. In order to ensure a page reaches the UE when paging optimisation is performed, the MME/SGSN/MSC shall page the UE at all CSGs which are in the UE's CSG subscription data and that advertise a TA/LA/RA where the UE may be camped on. This paging shall be performed regardless whether CSG subscription(s) that are stored by MME/SGSN/MSC are expired or not.
    - If an operator does not deploy OTA/OMA DM, paging optimization shall be disabled (and the HSS should delete expired CSG Ids directly when they expire, or are removed). FFS how to handle cases when home PLMN does not deploy OTA/OMA DM but the visited PLMN does (e.g., potentially the visited PLMN could disable paging optimisation for roamers).
- In addition, if the UE is in Connected mode at a CSG cell and the CSG timer expires or the CSG is removed from the subscription data, then the MME/SGSN/MSC shall perform S1/Iu release procedure with appropriate cause.

NOTE 5: It is FFS whether the HNB/HeNB first attempts to perform a handover of the UE to a suitable cell if a CSG timer expires or is removed. (See clause 6.3.2 for evaluation.)

NOTE 6: The S1/Iu release procedure will not cause the UE to update the Allowed CSG list.

Functionality in other entities:

- It is also possible for a potential CSG list server to inform the UE over OMA DM or OTA of a changed list of allowed CSG Ids, caused by the adding/removing/changing the expiration time for a CSG Id or by adding/removing CSG IDs.
    - An OTA/OMA DM update shall overwrite the entire Allowed CSG list
- In this case, the CSG list server shall indicate to the HSS (via an unspecified interface) whenever the Allowed CSG list on the UE has been updated via OMA DM or OTA, i.e., the HSS is aware which CSG Ids have been updated in the Allowed CSG list. When the CSG list server indicates to the HSS that a CSG ID is removed from UE list then the HSS removes that CSG ID from the subscription data.
- Only a successful OMA DM/OTA update shall remove the CSG Id from the HSS.

NOTE 7: The use of the NAS procedure at the MME/SGSN/MSC to remove a CSG ID from UE list will not result in the CSG Id being removed from the CSG subscription data at the HSS.

6.2 Release 8 and Release 9

6.2.1 Architectural issue - Network interface scalability

6.2.1.1 Description

With the introduction of H(e)NBs, the core network elements (e.g. SGSN, GGSN, MSC in UTRAN and MME, SGW in E-UTRAN) may now be required to handle a significant number of associations with H(e)NBs. The increased number of H(e)NBs may impact the number of SCTP associations and application layer associations that need to be handled by the core network elements.

6.2.1.2 Solutions

6.2.1.3 Evaluation

6.2.2 Architectural issue - Paging optimization

6.2.2.1 General

6.2.2.1.1 Description

The support of paging optimization is still under discussion in Rel-8 for Closed access mode H(e)NBs. Paging optimization may become even more important with the introduction of Hybrid and Open access modes since there may now be many more suitable cells on H(e)NBs where a UE may be paged.

6.2.2.1.2 Solutions

6.2.2.1.2.1 Solution 1

For two kinds of HeNB deployment architecture, the solutions of paging optimization for closed mode HeNB are as follows:

- HeNB directly connect to MME

  The CSG id(s) and access mode of the HeNB can be transferred to MME when HeNB initiates S1 set up procedure. If the configured CSG id(s) and access mode of the HeNB are changed, HeNB could initiates eNB configuration update procedure to update the configuration data stored in MME. MME can know the access mode of HeNB and has the relationship between HeNB and CSG id(s). When MME initiates paging procedure, it sends paging message to the close mode HeNBs which have the TAI in the UE's TAI list and the CSG id in the UE's allowed CSG list.

- HeNB connect to MME via HeNB GW

  In this case, CSG id(s) and access mode of HeNB does not need to be transferred to MME when HeNB initiates S1 set up procedure. The HeNB GW which acts as the concentrator of HeNBs could store the access mode and the relationship between HeNB and CSG id(s), the HeNB GW can perform the paging optimization. When MME initiates paging procedure, it provides the UE's allowed CSG list in paging message and sends the message to HeNB GWs which have the TAI in the UE's TAI list. The HeNB GW could forward the paging message to appropriate closed mode HeNB.

When the HNB is deployed in the network, the paging optimization can use the same mechanism above as when the HeNB connect to MME via HeNB GW case.

6.2.2.1.3 Evaluation

6.2.2.2 Sub-issue 1 - CSG Id list usage when HeNB Gateway is deployed

6.2.2.2.1 Description

Paging is generally performed in the TA(s) that the UE has in its TA list. Paging optimization can be performed by sending page messages only to the HeNBs in the TAs supporting the CSG Ids that the UE being paged has in its allowed CSG list. The node implementing paging optimization need to have knowledge of the CSG Ids handled by a certain HeNB.

As defined in TS 36.413 version 8.4.0, CSG Id list is sent from the HeNB to MME to inform the MME which CSG ID(s) is served by the Home eNB. MME can use this information when deciding which HeNBs to send page messages to, and MME performs the paging optimization.

If HeNB Gateway is deployed the following issue need to be handled:

- If the HeNB Gateway shall transfer all CSG Ids, related to all Home eNBs served by the Home eNB Gateway, to MME the defined maximum length (256) of the CSG Id list is far too short.

6.2.2.2.2 Solutions

6.2.2.2.2.1 Solution 1

The CSG ID list size does not change from Rel-8. A solution is to keep the list of CSG Ids in the HeNB Gateway and only transfer the TAIs served by the HeNB Gateway to MME. This means that the HeNB Gateway performs the paging optimization. Paging is then performed on tracking area level in the MME and the HeNB Gateway selects which CSG to forward the paging to.

This means that the CSG Id List is not transferred in the S1 SETUP REQUEST or in the ENB CONFIGURATION UPDATE messages from HeNB Gateway to MME. The CSG Id List is only transferred in the S1 SETUP REQUEST or in the ENB CONFIGURATION from HeNB to HeNB Gateway.

6.2.2.2.3 Evaluation sub-issue1

6.2.3 Architectural issue - Basic CSG access control

6.2.3.1 Description

According to Rel-8 baseline, there are three cases for basic CSG access control:

- For non-CSG capable UEs accessing a HNB, access control is performed by the HNB GW and optionally by the HNB based on subscription information configured on HNB/HNB GW. CN nodes do not perform CSG access control in this case;
- For CSG capable UEs accessing a HNB, CSG access control is performed by the CN nodes;
- For UEs accessing a HeNB, CSG access control is performed by the CN nodes.

In Rel-8, there is closed access mode HNB/HeNB.

- Closed CSG cells only allow the UEs of corresponding CSG subscribers to access. When a UE requests for access via a closed CSG cell, the network shall perform CSG access control for this UE.

In Rel-9, there are two additional access modes of HNB/HeNB, i.e. open access mode and hybrid access mode.

- All UEs can access via an open cell. The network does not perform CSG access control for the UEs accessing open cells of HNB/HeNB.

- Hybrid CSG cells allow all UEs to access. This is same as open cells or macro cells. If the network knows the access mode is hybrid, the network will not perform CSG access control for the UE.

The following aspects should be addressed by all proposed solutions:

- Besides the UE's CSG subscription data, what information is used by the CN nodes to perform CSG access control and how the CN nodes get this information?
- How does CN node know whether it needs to perform CSG access control for a UE? Particularly in HNB case, whether
  - CSG access control is performed by both the SGSN and the MSC/VLR;
  - Or CSG access control is performed by either the SGSN or the MSC/VLR and which CN node performs CSG access control.

6.2.3.2 Solutions

6.2.3.2.1 Solution1

CSG access control regarding access mode:

- When a UE requests for access via a closed CSG cell, the network performs CSG access control for this UE.
- When a UE requests for access via an open cell or hybrid CSG cell, the network does not perform CSG access control for the UE.

In HNB case:

For non-CSG capable UEs, the HNB GW and optionally the HNB performs CSG access control based on subscription information (e.g. an allowed IMSI list of a HNB/CSG).

For CSG capable UEs, the SGSN and the MSC/VLR perform CSG access control independently when Iu connection is setup for the UE according to the implicit indication by HNB GW.

The HNB GW implicitly indicates to the SGSN and the MSC/VLR whether they need to perform CSG access control as follows:

- For CSG capable UEs the HNB GW always accepts the registration request and sends both the access mode and CSG ID to the SGSN/MSC/VLR when Iu connection is setup for the UE. The SGSN/MSC/VLR performs CSG access control for the UE based on received access mode and CSG ID information.
- For non-CSG capable UEs, the HNB GW and optionally the HNB performs CSG access control for the UE. If the UE is allowed to access this HNB, the HNB GW accepts the registration request and sends only the CSG ID to the SGSN/MSC/VLR when Iu connection is setup for the UE. Then the SGSN/MSC/VLR does not perform CSG access control for the UE as the access mode parameter is not sent by the HNB GW.

In HeNB case:

The MME always perform CSG access control for UEs accessing via a CSG cell. So the access mode and CSG ID is sent to the MME by the HeNB (or by the HeNB GW when deployed) during S1 connection is setup for the UE. The MME performs CSG access control based on received access mode and CSG ID information.

Advantages of this solution:

- Do not add additional parameter to indicate the CN node to perform access control.
- Consistent for CSG access control in CS only, PS only and CS&PS cases.

6.2.3.3 Evaluation

6.2.4 Architectural issue - HNB support for legacy CN

6.2.4.1 Description

As outlined in the current TS 25.467, access control for CSG capable UEs is performed by the core network, and the HNB GW should always accept a CSG capable UE's registration request and assign a context ID in the response.

There are three possible HNB deployment scenarios as following:

- Use case 1: All the CN nodes which the HNB GW are connected to are release 8;
- Use case 2: All the CN nodes which the HNB GW are connected to are legacy;
- Use case 3: The CN nodes which the HNB GW are connected to include some legacy CN nodes and some release 8 CN nodes.

If the HNB GW is connected to a pre-R8 core network, the legacy CN node is not required to perform access control for CSG capable UEs. So in this scenario, if the HNB GW/HNB does not perform CSG access control, a rogue UE announcing it is CSG capable can access any HNB which is connected to a pre-R8 CN node.

6.2.4.2 Solutions

6.2.4.2.1 Solution1

The following solution is based on the reasonable assumption that the HNB GW can be configured (e.g. via management system) with the version of the CN nodes which the HNB GW is connected to.

If the CN node version information configured in the HNB GW indicates pre-R8 CN, the HNB GW performs access control for all UEs including CSG capable UEs and non-CSG capable UEs.

NOTE: This also allows flexibility for operators to use the same access control solution for CSG capable UEs as for non-CSG capable UEs by configuration.

If the CN node version information configured in the HNB GW indicates mixed pre-R8 and R8 CN, e.g. the SGSN is updated to R8 with CSG function, but the MSC/VLR is still pre-R8. There are two possible alternatives:

- Alternative 1: The HNB-GW selects a R8 CN node based on configured information and the selected CN node performs access control for a CSG capable UE.
- Alternative 2: If the selected CN node is R8, the selected CN node performs access control for a CSG capable UE; if the selected CN node is pre-R8, the HNB GW performs access control for CSG capable UE.

If the CN node version information configured in the HNB GW indicates R8 CN, the selected CN node performs access control for a CSG capable UE.

6.2.4.3 Evaluation

6.3 Release 9

6.3.1 Architectural issue - Time period control

6.3.1.1 Description

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.

6.3.1.2 Solutions

6.3.1.2.1 Solution 1

CT WG4 has agreed that time period is a CSG-Subscription-Data stored in HSS, which is described in TS 29.272. When the MME/SGSN/MSC receives CSG-Subscription-Data from the HSS, the time period information is also sent to the MME/SGSN/MSC.

Either the HSS or the MME/SGSN/MSC can perform a check on the expiry of the time period during which a subscriber is granted access. However, considering the critical role in the mobile network of the HSS, it is not advisable to use the HSS to perform such check. Furthermore, in Release 8 it has been agreed that the MME/SGSN/MSC is the entity where the access control function is implemented. It is therefore natural to assume that the check on the time period during which the subscriber is granted access is performed by the MME/SGSN/MSC.

6.3.1.2.2 Solution 2

TS 23.008 states that the Allowed CSG list sent by the HSS/HLR to the MME, MSC/VLR and SGSN includes the expiry time.

It is proposed that the UE should be informed of the expiry time as follows:

- **Allowed CSG list:** The expiry time should be included in the Allowed CSG Management Object in OMA DM or OTA.
- **User CSG list:** The expiry time should be included in the MME, MSC/VLR and SGSN NAS signalling response to the Attach, Detach, Location Registration procedures (LAU/RAU/TAU) since a UE may also add a CSG to the User CSG list via manual CSG selection.

NOTE: For Rel-8 there is no User CSG list.

In addition it is proposed that the H(e)NB be informed of the expiry time for a UE that accesses or performs a handover to the CSG cell

The MME, MSC/VLR and SGSN should remove the CSG entry once the membership time has expired.

In both idle mode and connected mode the UE shall remove the CSG from the User CSG list when the timer expires.

NOTE: If the UE has the CSG in the User CSG list then adding the expiry time to the NAS procedures means that the MME, MSC/VLR and SGSN can safely delete the CSG entry in the Allowed CSG list once the membership expires because the UE will be aware that the membership has expired.

If the UE is in idle mode at a CSG cell for which the timer expires, the UE shall reselect to another suitable cell.

The disadvantages of this solution are as follows:

- UE impacts, i.e., the UE needs to keep an accurate time to delete entries correctly
- This solution does not solve the scenario for how to update the UE's CSG list when the UE is a permanent CSG member and is removed from the CSG. Based on the solution adopted for this case, the need for this solution will be revisited.

6.3.1.3 Evaluation

6.3.2 Architectural issue - Diversion of established communications

6.3.2.1 Description

It shall be possible to divert established communications via a CSG cell to a non-CSG cell. This procedure is applicable in the following cases:

- in hybrid access mode, when services cannot be provided to a CSG member due to a shortage of HNB/HeNB resources.
- at the expiry of the time period for temporary CSG members.

6.3.2.2 Solutions

6.3.2.2.1 Solution 1

When the time period expires, the temporary member is no longer allowed to access the operator's network via the current CSG cell. The temporary member may however still be permitted to access the operator's network via a non-CSG cell. In order to assure continuity of the established communications, when the time period expires it shall be possible to invoke a handover procedure to move the established communications to a permissible cell.

Similarly, for the hybrid access mode, it shall be possible to perform a handover from the CSG cell in use by a non CSG member to a non-CSG cell.

6.3.2.2.2 Solution 2

If the UE is in connected mode at the CSG cell for which the timer expires, the following procedures are proposed:

- The MME, MSC/VLR or SGSN should communicate the expiry time to the CSG cell when the UE connects to that CSG cell
- The CSG cell should try to handover the UE to a suitable cell before the timer expires.

NOTE: In Rel-9 the CSG cell may also find a CSG cell for another suitable CSG to handover the UE to as well.

- If the CSG cell cannot handover the UE, then the MME shall perform a S1 Release procedure when the timer expires. An equivalent procedure may be performed by the MSC/VLR or SGSN. In this case the UE will go to idle mode, remove the CSG ID from the User CSG list if present and access at another suitable cell if possible.

6.3.2.3 Evaluation

6.3.2.3.1 Diversion of established communications at the expiry of the time period for temporary CSG members

If handover is used to divert communication from a CSG cell at the expiry of the time period for temporary CSG members then the following functionality applies:

Functionality in MME/SGSN/MSC at the expiry of the time period for temporary CSG members:

- The MME, SGSN and MSC shall send an S1/Iu release to the H(e)NB where the UE is connected if the timer has expired for temporary CSG members at a closed CSG cell.

Functionality in CSG cell in H(e)NB at the expiry of the time period for temporary CSG members:

- If the UE is in Connected mode at a CSG cell and the CSG cell receives an S1/Iu release from the MME/SGSN/MSC that the CSG Id is expiring, then a closed access CSG cell should try to handover the UE to a suitable cell before the timer expires.
- If handover is not possible then the CSG cell shall release the connection.

NOTE: Handover may not always be possible based on the surrounding coverage of the CSG cell.

6.3.2.3.2 Diversion of established communications from a hybrid CSG cell when services cannot be provided to a CSG member due to a shortage of HNB/HeNB resources

If handover is used to divert communication from a hybrid CSG cell when services cannot be provided to a CSG member due to a shortage of HNB/HeNB resources then the following functionality applies:

Functionality in MME/SGSN/MSC for Hybrid access mode H(e)NBs:

- The MME, SGSN and MSC shall inform the H(e)NB whether the UE is a member of the CSG for Hybrid access mode H(e)NBs.

Functionality in CSG cell in H(e)NB for Hybrid access mode H(e)NBs:

- The H(e)NB may handover a UE that is not a member of the CSG to a suitable cell due to a shortage of H(e)NB resources.

6.3.3 Architectural issue - Number limit

6.3.3.1 Description

The network operator and/or the HeNB owner under the supervision of the network operator shall be able to set a maximum limit to the number of UEs with granted access to a given CSG cell. This limit is a static setting which can only be changed/set during configuration or maintenance.

6.3.3.2 Solutions

6.3.3.2.1 Solution 1

Two scenarios need to be considered with regards to the number limit requirement:

1. The CSG consists of a single cell. In this scenario, the HeNB may perform the number limit control. In the case where all the UEs access same MME/SGSN/MSC via the HeNB, then the MME/SGSN/MSC may perform the number limit control.

2. The CSG consists of more than one HeNB. In this scenario, the HeNB can not perform the number limit control for the CSG. In order for the MME/SGSN/MSC to be able to perform the number limit control for the CSG, it is necessary that all UEs in the CSG access the same MME/SGSN/MSC.

As the HeNB GW is an optional entity, (as agreed in architecture for HeNB deployments in RAN3), the number limit control for CSG cannot be performed in HeNB GW. Thus the control of maximum limit to the number of UEs with granted access to the CSG needs to be performed in MME/SGSN/MSC.

6.3.3.3 Evaluation

6.3.4 void

6.3.5 Architectural issue - Shared network aspects

6.3.5.1 Description

If CSG-Id functionality shall be able to co-exist with shared networks or not, and if it shall, what implications can it have on the architecture?

If so, whether and how a single HNB supports subscribers from multiple PLMNs of the same country?: Since a CSG Id is unique per PLMN, and the CSG Id for a certain PLMN is stored in the subscribers HSS for this PLMN, it is not obvious how to treat a CSG Id for a PLMN if there is no HSS for this PLMN (and the RAN-PLMN do not have a HSS in a shared network?). It needs to be studied how the usage of CSG Id would work in a shared network scenario, since the RAN may have a separate PLMN-id compared to the PLMN-Id of the CN. If a H(e)NB owner adds a CSG member into its CSG list, it seems necessary to use the PLMN-Id for the RAN, since the same RAN may be used by two different PLMN-Ids from a CN perspective. However, there is no one-to-one relation between the PLMN-Id of the shared RAN and a HSS, which is an issue when the H(e)NB owner shall add a CSG member into a HSS.

6.3.5.2 Solutions

6.3.5.3 Evaluation

6.3.6 Architectural issue - In-bound H(e)NB handover support

6.3.6.1 Description

In-bound connected mode handover to H(e)NB for a UE was not supported in Rel-8 due to time constraints but is a requirement for Rel-9 as stated in TS 22.220 [2]:

- With the exception of GERAN to E-UTRAN handover, it shall be possible to support service continuity when UE moves from a non-CSG cell to a CSG cell.
- It shall be possible to support service continuity when UE moves from a CSG cell to a non-CSG cell or another CSG cell.

Proper implementation of in-bound connected mode handover requires the following issues to be resolved in the core network:

- **Connected mode access control:** How to perform access control for an in-bound handover to a H(e)NB when the H(e)NB is operating as a closed CSG cell, i.e. to ensure the UE is performing handover to a suitable CSG cell.
- **Various access mode supported:** How to perform access control correctly when H(e)NB is operating as a hybrid/open CSG cell, i.e. to ensure the UE is performing handover to a suitable CSG cell.
- **How to route S1AP message to target HeNB GW/HeNB:** how to let MME route S1AP message to target HeNB GW/HeNB for an Inbound handover to a H(e)NB.

Editor's note: RAN solution for in-bound handover to CSG cells has not been decided yet.

6.3.6.2 Solutions

6.3.6.2.1 Solution 1: Including the Allowed CSG list in the *Handover Restriction List* IE

As currently defined, the *Handover Restriction List* IE is included in various S1-AP and X2-AP messages such as INITIAL CONTEXT SETUP REQUEST and HANDOVER REQUEST, and it is used by the source eNB to determine a target cell based on equivalent PLMNs and forbidden TA/LAs for the UE.

To support in-bound connected mode handover, it is proposed to expand the *Handover Restriction List* IE to also include the Allowed CSG list of the UE. This allows the source eNB to use this information to determine if a target CSG cell is suitable for handover.

NOTE 1: It is a fundamental requirement for network controlled handover for the source eNB to know the target (H)eNB's identity and certain other parameters in order to prepare the target cell for handover. TS36.300 sec 22.3.3 and 22.3.4 describes the method by which the source eNB automatically discovers any neighbouring target cells via the Automatic Neighbour Relation (ANR) Function using UE measurement reports. In addition O&M in TS 32.511 manages which cells the eNB may establish neighbour relations with, i.e., O&M may limit the cells that the source eNB may perform a handover with. In ANR, the UE reports the global Cell ID, tracking area code and all PLMN IDs that have been detected. By extending the ANR in Rel-9 to support in bound handover to HeNBs, the UE may also report the access mode (closed/hybrid/open) and the CSG ID. The source eNB will then have all the information needed to determine if the target CSG cell is suitable for handover.

NOTE 2: This solution is based on an assumption that ANR Function is extended to let the UE reports the access mode and the CSG ID to the source eNB. But this assumption has not been agreed by RAN and other alternatives remain possible.

The advantages of this approach include:

- Allows the source eNB to efficiently determine whether a target cell is suitable for handover without any extra messages.
- In the case a target cell is a hybrid access mode HeNB, the source eNB would know whether the UE belongs to the CSG and hence may prefer handover of the UE to the target cell.
- No changes to any of the existing handover procedures.
- Forward compatible for instance if the X2 interface is included in Rel-9 or later HeNB implementations.

NOTE 3: Any method that requires the MME to perform the check to determine if the target cell has a CSG ID in the UE's Allowed CSG list will (a) require an extra handshake in order to perform X2 based handover and (b) requires the MME to perform this check for S1 based handover when the source eNB sends a HANDOVER REQUIRED message which may mean a greater processing at the MME and extra delay when the source eNB requests a handover to a non-suitable CSG cell.

6.3.6.2.2 Solution 2: CSG Access control in the Core Network with support from the source RAN node

In this solution the Core Network elements (MME/SGSN/MSC) performs the access control during the in-bound handover to HNB/HeNB. The Source NB/eNB/HNB/HeNB sends the target CSG ID and access control mode of the target HNB/HeNB to the Core Network in the handover request, and the Core Network performs access control based on the UE allowed CSG list as the same as the normal attach procedure. If the access control fails the Core Network shall return an error cause to the source NB/eNB/HNB/HeNB to indicate the reason why the handover failed (e.g. the target CSG id is not in the UE allowed CSG list). The source NB/eNB/HNB/HeNB may select another target cell and send handover request again.

6.3.6.2.3 Solution 3: CSG Access control in the Core Network with support from the target RAN node

For this solution we assume the following:

- As the Core Network node (MME/SGSN/MSC) performs CSG access control during in-bound handover. The NB/eNB/HNB/HeNB does not need to perform CSG access control thus the Allowed CSG List is not needed to be transferred to NB/eNB/HNB/HeNB.
- The source NB/eNB/HNB/HeNB does not have the neighbour CSG cells' configuration.
- CSG ID and access mode provided by the UE via the source NB/eNB/HNB/HeNB can not be trusted.

When the Core Network node (MME/SGSN/MSC) receives message from source RAN node indicating handover is required, the CN node gets the CSG ID and access mode of the target cell directly from the target HNB/HeNB/HNB GW/HeNB GW. Then the CN node performs the access control during the in-bound handover to HNB/HeNB.

NOTE: The CN node can use current handover preparation procedure to get the information from the target HNB/HeNB. Or a new pair of messages can be defined to get the information from the target HNB/HeNB.

The advantages of this approach include:

- No impact or requirement for access control either on the behaviour of source RAN node or on the behaviour of the UE.
- The CSG ID and access control mode of the target cell are validated by the target HNB/HeNB. Thus this solution mitigates the risk for the UE to hand off on a CSG cell for which the UE is not allowed.

Editor's note: It is FFS how to perform access control if the MME/SGSN/MSC is relocated during the handover procedure.

6.3.6.3 Evaluation

6.3.7 Architectural issue - Open and hybrid access mode H(e)NB support

6.3.7.1 Description

There are three modes for H(e)NBs for Rel-9, namely:

- **Closed access mode:** H(e)NB operates as a CSG cell.
- **Hybrid access mode:** H(e)NB operates as a CSG cell where at the same time, non-CSG members are allowed access.
- **Open access mode:** H(e)NB operates as a normal cell, i.e. non-CSG cell.

There are four main issues related to support of hybrid mode:

- management of the UE's Allowed CSG list
- preferred resource allocation for CSG members by H(e)NBs that operate in hybrid mode.
- indicating the access mode to other network entities
- diversion of established communication for a non-CSG member when services cannot be provided to a CSG member due to a shortage of HNB/HeNB resources

6.3.7.2 Sub-issues

6.3.7.2.1 Sub-Issue 1 - Management of the UE's Allowed CSG list

6.3.7.2.1.1 Description

The following requirements related to hybrid CSG cells have been agreed by SA WG1:

- Manual and automatic CSG selection applies to Hybrid access mode H(e)NBs.
- Upon registration the network shall indicate whether the UE is a member of the CSG. If the UE is a member of the CSG, the UE shall add the CSG identity to the User CSG list, unless that identity is already present in the list.

The management of the UE's allowed CSG list for closed mode uses an implicit indication of CSG membership with every mobility management transaction between UE and network. Access to hybrid mode H(e)NBs is allowed for every UE/user. Therefore compared to closed mode CSG list management existing mobility management procedures cannot implicitly provide additional functionality about CSG membership when hybrid mode is used according to the stage 1 requirements.

6.3.7.2.1.2 Solutions

6.3.7.2.1.2.1 Solution 1: Manual CSG selection and UE Allowed CSG list management

For open access mode, the H(e)NB is not a CSG cell, so there is no impact on CSG list management.

For hybrid access mode, we propose to define a new accept cause value to indicate whether the UE is a member of the CSG advertised by the hybrid cell for attach and location area updating procedures (LAU/RAU/TAU). The MME, MSC/VLR or SGSN includes the accept cause in the NAS signalling response to indicate that the UE is a member of a CSG cell. The UE then updates the User CSG list based on the specified accept cause value if it is not already present in the CSG list.

Editor's note: It is FFS whether a UE's knowledge that it is a member of a CSG impacts any UE behaviour, and therefore whether this new cause value is needed.

6.3.7.2.1.2.2 Solution 2: UE Allowed CSG list management by OTA/OMA DM

It is proposed to add any CSG IDs of hybrid mode cells to the UE list of allowed CSGs only by OTA/OMA DM. The acceptance of mobility management procedures (Attach, LAU, RAU, TAU) does not add any CSG ID to the UE's allowed CSG list when these procedures are performed via a CSG cell that indicates hybrid mode. If the network rejects a mobility management procedure in a hybrid mode CSG cell with a CSG related cause value the CSG ID is removed from the UE list of allowed CSGs.

It may be considered as a drawback that a CSG member's UE, until its allowed CSG list is updated by OTA/OMA DM, will not perform the preferential selection of that CSG. As a non-member the UE is able to select that cell automatically because any UE gets access to a hybrid mode cell.

The advantage of this solution is that hybrid mode CSG support can be introduced without upgrading the large number of cases of successful mobility management signalling scenarios between UE and network for differentiating whether it is CSG related or not.

6.3.7.2.1.3 Evaluation

Two solutions are proposed for this issue. To simplify the implementation, solution 2 is adopted. It means that adding a CSG ID of hybrid mode cells to the UE's local Allowed CSG List is performed only by OTA/OMA DM.

6.3.7.2.2 Sub-Issue 2 - Admission control and rate control for hybrid access mode

6.3.7.2.2.1 Description

If a HNB/HeNB operates in hybrid access mode, to minimise the impact on CSG members of communications established by non-CSG members, it shall be possible for the network to reduce the data rate of established PS communication of non-CSG members. It shall also be possible for the network to follow different admission control policies for CSG and non-CSG members.

The preferred resource allocation for CSG members by hybrid mode H(e)NBs does not require any enhancements of the signalling between UE and network. The mobility management procedures are not affected by it.

6.3.7.2.2.2 Solutions

6.3.7.2.2.2.1 Solution 1

As CSG related access control are performed in MME/SGSN/MSC, it is appropriate for the MME/SGSN/MSC to use different admission control thresholds for CSG and non-CSG members when the CSG operates in hybrid mode and to be capable of reducing data rate of PS communication established by non-CSG members.

6.3.7.2.2.2.2 Solution 2

When the UE context is established in the H(e)NB, the MME, SGSN or MSC provides an indication to the H(e)NB whether the UE is a CSG member or not. Based on this information the H(e)NB performs differentiated admission control and rate control for CSG and non-CSG members.

Any additional information for differentiated handling of CSG and non-CSG members (i.e. admission thresholds and AMBR-like thresholds for non-CSG members) is configured locally in the H(e)NB per operator policy.

In case of changes of the CSG membership status (e.g. expiry of temporary CSG membership), it should be possible for the Core Network node to convey this change to the H(e)NB dynamically.

6.3.7.2.2.3 Evaluation

Two solutions are proposed for this issue. Solution 1 requires MME/SGSN/MSC to support additional admission control function and will cause frequent signalling on Iu/S1 interface. Thus solution 2 is adopted for the admission control issue for hybrid access mode H(e)NB.

6.3.7.2.3 Sub-Issue 3 - Indicating the access mode to other network entities

6.3.7.2.3.1 Description

Network entities use the CSG ID of the CSG cell to perform operations like access control at a CSG cell. The network entity performing these operations are already required to know the CSG ID of the H(e)NB to function correctly. What needs to be understood is how the access mode is also communicated to these entities?

6.3.7.2.3.2 Solutions

6.3.7.2.3.2.1 Solution 1: Indicating the access mode to other network entities

Network entities use the CSG ID of the CSG cell to perform operations like access control and paging optimization for the CSG cell. The network entity performing these operations is already required to know the CSG ID of the H(e)NB to function correctly.

If the access mode (closed/hybrid/open) is communicated along with the CSG ID, then the network entity will know how to treat the H(e)NB appropriately. A H(e)NB in open access mode does not have a CSG ID and only needs to communicate the access mode.

For example, for performing access control, the network entity will know whether to check if the CSG ID of the H(e)NB is in the UE's subscription data based on the reported mode of the H(e)NB. For closed mode the network entity needs to perform access control based on the CSG ID, while for open or hybrid access mode this check is not needed.

H(e)NB adds the H(e)NB access mode together with the CSG ID of the current CSG cell in RANAP/S1-AP signalling when UE initiates NAS message to access the network. The network entity uses these parameters to perform access control. HNB registration procedure is used to report the CSG ID(s) and the access mode of HNB to the HNB GW for paging optimization. Depending on whether HeNB GW is deployed, S1 setup procedure reports the CSG ID(s) and the access mode of HeNB to HeNB GW or the network entity for paging optimization.

NOTE: The details of indicating CSG ID and access mode of H(e)NB to network entity only cover solution 1.

6.3.7.2.3.3 Evaluation

As the R8 H(e)NB, which is in closed access mode, only reports its CSG ID to the core network, no access mode parameter is defined in R8, the core network shall regard the H(e)NB as closed access mode when the CSG ID is received without the access mode parameter.

When the access mode parameter is received along with the CSG ID, the network shall treat the H(e)NB according to the received access mode.

6.3.7.2.4 Sub-Issue 4 - Diversion of established communication for a non-CSG member

See section 6.3.2 for description, solutions and evaluation.

6.3.7.3 Evaluation

See clause 6.3.7.2.1.3, clause 6.3.7.2.2.3, clause 6.3.7.2.3.3,clause 6.3.2.3 for the evaluation of Allowed CSG List management, admission control, access mode and diversion sub-issues.

6.3.8 Architectural issue – CSG membership management (Rel-9?)

6.3.8.1 Description

TS 22.011, clause 8.3.1 contains the following requirement:

> "*The owner of the HeNB or HNB shall be able, under the PLMN operator supervision, to add, remove and view the list of CSG members. The consent of the invited member or guest shall be obtained before being added to the subscriber group.* "

It seems less attractive to let the H(e)NB owner directly contact an HSS to add, remove and view the list of CSG members, and therefore it seems required to have one or more intermediate entities between the H(e)NB owner and an HSS. If these entities, or any interfaces towards these entities, need to be specified by 3GPP is FFS. It can be noted that the interface between the H(e)NB owner in VPLMN and the HSS of the temporary guests HPLMN is an inter-PLMN interface, which seems to exclude proprietary solutions.

Issue: Shall any entity, or interface, used by the H(e)NB owner to add, remove and view the list of CSG members be specified by 3GPP, including interfaces to HSS?

6.3.8.2 Solutions

6.3.8.3 Evaluation

6.3.9 Support for Local IP Access

6.3.9.1 Description

This clause addresses the architecture issues related to support for Local IP Access (LIPA) to the home based network and to the Internet.

The requirements for support of LIPA to the home based network and to the Internet are defined in clause 5.1.7 and clause 5.1.8, respectively.

6.3.9.2 Solutions

6.3.9.2.1 Solutions covering both LIPA to the Internet and to the home-based network

6.3.9.2.1.1 Solution 1: Local IP Access solution based on traffic breakout performed within H(e)NB using a local PDN connection

6.3.9.2.1.1.1 Architectural principles

Common principles applying to both UMTS and EPS:

- Two PDN connections are assumed for simultaneous LIPA traffic and non-LIPA traffic.
- Pre-Rel-9 UEs that support Multiple PDN connections can simultaneously access LIPA and non-LIPA PDN connections.
- For LIPA traffic a Local P-GW function or Local GGSN function for EPS and UMTS, respectively is located within the H(e)NB.
- For non-LIPA traffic, P-GW/GGSN is located within the core network.
- Local IP access PDN can be identified by a well-defined APN.
- Mobility management signalling between UE and network is handled in the core network.
- Session management signalling (Bearer setup, etc.) for non-LIPA traffic terminates in the core network.
- Before LIPA PDN connection is established, the UE is authenticated, authorized and registered by the core network.

Additional principles applying to UMTS only:

Additional principles applying to EPS only:

- LIPA session management (LIPA PDN Connectivity establishment, Bearer management, etc.) is performed in the core network.

6.3.9.2.1.1.2 Open architectural issues

This section lists the open architectural issues, which have been identified for this solution.

NOTE: Whether further open issues exist is FFS.

Common open issues applying to both UMTS and EPS:

- Whether the H(e)NB provides Legal Intercept (LI) functionality.
- Whether and how to assist the backhaul operator to perform legal intercept (e.g., by making core network aware of IP address assigned to LIPA PDN connection).
- Whether Mobility (to macro-network and another H(e)NB) is supported/required for LIPA traffic.
- Whether QoS for LIPA traffic is based on static policies (no Gx to H(e)NB).

Open issues applying to UMTS only:

- Location of LIPA session management.

Open issues applying to EPS (LTE and S4-based UMTS) only:

- Location, number and possible subset of S-GW functions (two S-GWs (in HeNB and core network) vs. one S-GW with relocation).
- S11 interface to the HeNB to manage bearer setup for LIPA.

6.3.9.2.1.2 Solution 2 – Single UE IP address with LIPA at H(e)NB

6.3.9.2.1.2.1 Architectural principles

- UEs are only required to activate one PDN connection for LIPA and Non-LIPA traffic.
- H(e)NB has the ability to drag/insert the LIPA traffic from/into PDP context/bearers based on destination address.
- There is a NAT inside H(e)NB to ensure returning LIPA traffic reaches H(e)NB despite topologically incorrect source address.
- Pre-Rel9 UEs that support single PDN connections can simultaneously access LIPA and Non-LIPA.

6.3.9.2.1.2.2 Open Issues

For this solution, the only requirements are NAT and routing functionalities for the H(e)NB. The solution has the following issues as FFS:

- How to provide Internet service continuity when a UE hands over to a macro cell is FFS, if this function is required.
- It is FFS if the LIPA function needs to support NAT traversal for other home applications.
- It is FFS on addressing the possibility that the private IPv4 address of the home IP devices conflict with operator's services which using private IPv4 addresses.
- Whether it is necessary or not and how to block access to Local IP access for non-CSG users at a hybrid H(e)NB is FFS.
- It is FFS whether paging the UE from the H(e)NB requires a S-GW function to reside in the H(e)NB.
- How to do IPv6 prefix translation (NAT66) is FFS.

- How does the routing policy configured in the H(e)NB work for roaming CSG members, given that the H(e)NB does not know whether the destination address belongs to the IP services network of the roaming CSG member's HPLMN. How does the home operator enforce its routing policy?

6.3.9.3 Evaluation

6.3.10 void

6.3.11 Architectural issue - Support of Emergency Services

6.3.11.1 Description

For the UE access network via CSG, if the UE indicates to access network for emergency calls or handover for emergency call, CSG access control restriction shall be removed.

6.3.11.2 Solutions

6.3.11.2.1 Solution 1

If the CSG ID of the H(e)NB is not in the UE Allowed CSG List and UE camp on this H(e)NB, UE is in the limited service state. In that case besides the normal emergency process,

- When Emergency Attach Request is received, the MME/SGSN shall not reject it due to CSG access control restriction.
- When Emergency Service Request is received, the MME/SGSN/MSC shall not reject it due to CSG access control restriction.
- When Emergency PDN connection Request is received, MME/SGSN shall not reject it due to CSG access control restriction.
- When UE have emergency bearer services and TAU/RAU is triggered, MME/SGSN shall not reject it due to CSG access control restriction.

It is FFS how to support emergency service handover if the target H(e)NB CSG ID is not on the UE allowed CSG list.

6.3.11.3 Evaluation

6.4 Release 10

6.4.1 Architectural issue - Storage of CSG ID for temporary & roaming CSG members

6.4.1.1 Description

The conclusion of the CT WG4 Rel-8 work is that all allowed CSG Ids for a certain subscriber are stored in the HSS of the subscribers HPLMN. The storing of a CSG Id announced by a H(e)NB in VPLMN, requires that the HPLMN of the subscriber has a roaming agreement with the VPLMN, and that the HPLMN supports storing of CSG Id from a VPLMN.

Another conclusion is that a certain CSG Id may be found in more than one HSS, since a H(e)NB owner in one PLMN may invite persons from several PLMNs to use the CSG Id announced by the H(e)NB.

The following definitions apply to CSG members:

Temporary CSG Member: A member of a CSG for which there is an associated expiration time. When the time period expires, the CSG shall no longer be considered to be available to provide services, except for emergency calls.

Permanent CSG Member: A member of a CSG for which there is no associated expiration time.

Home CSG Member: A member of a CSG where the CSG is associated with the HPLMN. A Home CSG Member may be a Temporary CSG Member or a Permanent CSG Member.

Roaming CSG Member: A member of a CSG where the CSG is associated with a VPLMN. A Roaming CSG Member may be a Temporary CSG Member or a Permanent CSG Member.

Permanent and temporary CSG members may have their CSG IDs stored in HSS subscription data as defined in TS 29.272. A user's subscription has separate CSG ID lists for every PLMN where the user has CSG memberships.

The above implies two different types of CSG members, (Roaming and Home CSG members).

It may cause excessive load for the HSS to handle temporary CSG memberships, especially for short lived membership. For this reason, investigation for appropriate solution is needed. Additional consideration is also required for roaming scenarios.

Editor's Note: There needs to be further clarification whether there are two types of Temporary CSG members based on whether the member is stored as subscriber data in the HSS.

6.4.1.2 Solutions

6.4.1.2.1 Solution 1: Storage of CSG ID for temporary CSG members

A temporary CSG member can be either in non-roaming or roaming situation, depending on whether his PLMN is the same or different with the PLMN to which the H(e)NB connects. Therefore, the term "temporary CSG members" in this clause applies to both non-roaming and roaming CSG members.

Whereas permanent CSG members have their CSG IDs stored in the HSS (a separate 'Allowed CSG ID list' for every PLMN where the user has CSG memberships), this solution assumes that the information relative to the temporary CSG members is stored in the MME/MSC/SGSN (or MME/MSC/SGSN pool) to which the H(e)NB connects.

The information relative to temporary CSG members is stored in a CSG ID-specific context in the CN node (i.e. MME, MSC or SGSN) and is referred to as the "Temporary CSG Member list".

The "Temporary CSG Member list" is maintained in the CN node even when the latter contains no UE-specific context for a temporary CSG member.

The access control in the CN node is performed in two steps:

1) the CN node checks whether the CSG ID of the H(e)NB is contained in the "Allowed CSG ID list" fetched from the HSS;

2) if the previous step fails, the CN node checks whether the user identity is contained in the "Temporary CSG Member list" stored in the CSG ID-specific context.

The H(e)NB owner is able to add or delete specific user IDs to/from the 'Temporary CSG Member list' that is used by the CN node to perform access control. In addition to specifying access to the CSG, the H(e)NB owner also has the ability to specify additional criteria for the visiting user, such as the length of allowed access. The requested length of allowed access may be capped by statically provisioned maximum duration value in the CN node.

To enable the dynamic update of the 'Temporary CSG Member list' at the local CN node, the H(e)NB contains an "access provisioning server" functionality and exhibits a secure interface to the H(e)NB owner (e.g. a web-based interface secured with any kind of locally configured credentials). The collocation of the 'access provisioning server' with the H(e)NB permits the re-use of existing interfaces between the H(e)NB and the CN node.

Specifically for the HeNB case, when the HeNB owner requests addition of a temporary CSG member, the "access provisioning server" in the HeNB triggers the S1 ENB CONFIGURATION UPDATE procedure to inform the MME (or all the MMEs in the pool) about the new temporary member. When the temporary membership expires, the MME triggers the S1 MME CONFIGURATION UPDATE procedure to inform the HeNB that the visitor's membership has expired.

Equivalent Iu procedures are used for the HNB case.

The CN node may reject the H(e)NB owner's request for addition of a temporary CSG member. While it is impossible to make fine grained decisions based on the visitor's subscription profile (because the latter is not consulted during the process of member addition), the rejection decisions could be based on criteria such as the PLMN identity owning the visitor's subscription or the number of temporary members admitted in the CSG cell at the same time.

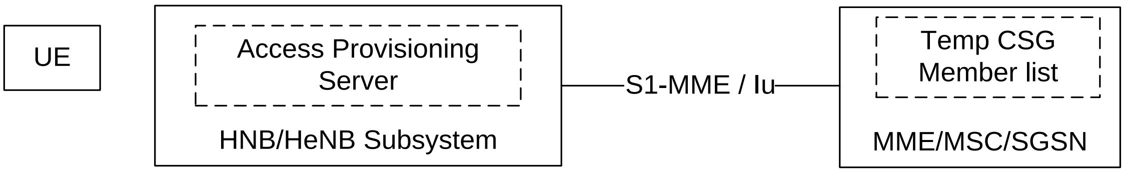

Figure 6.4.1.2-1: Location of the Access Provisioning Server and the Temporary CSG Member list

Editor's note: It is FFS how the Temp CSG Member list is restored when the CN node is restarted.

Editor's note: In scenarios where the same CSG ID is shared by H(e)NBs that are controlled by multiple CN node pools, the "Temporary CSG Member list" information specific to this specific CSG ID needs to be stored in all CN node pools. It is FFS whether such scenarios represent a valid use case.

6.4.1.2.2 Solution 2

This solution allows CSG managers to add and remove subscriber to their CSG memberships through a CSG Membership Management Server. How CSG managers access the CSG Member Mgmt Srv (e.g. through a Web interfaces) is considered outside the scope of this specification and left to the operator.

Upon a change of a CSG (i.e. when a CSG manager adds or removes a UE from its CSG), the CSG Member Mgmt server will update the allowed CSG list of the added or removed subscriber in its HLR/HSS.

In order to manage the CSG membership of a roaming UE, the CSG Member Mgmt Srv in the VPLMN must be able to update the HLR/HSS in the HPLMN via a standardized C2 interface.

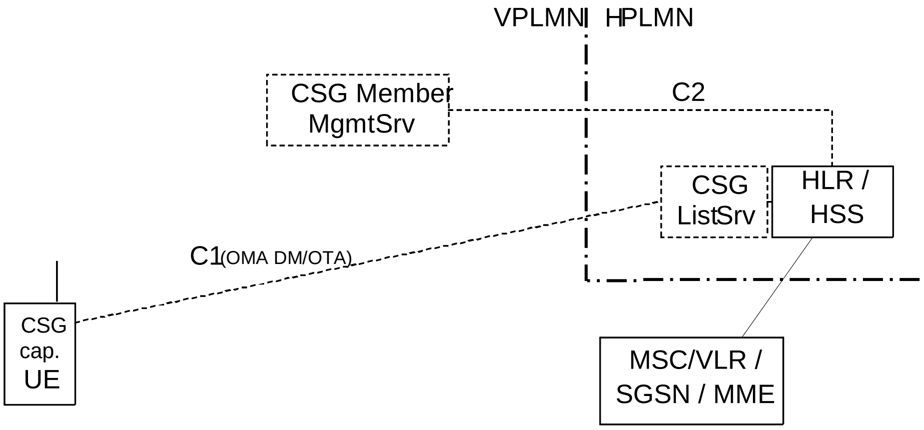

Figure 6.4.1.2.2-1: Solution 2

NOTE: The protocol on C2 is FFS. Whether one of the Rel-8 roaming interfaces (e.g. SWd) can be re-used is FFS.

This solution enables access control based on CSG information in a common way for both temporary and permanent CSG members.

The advantage of this solution is that the update of the subscriber's allowed CSG lists in the HLR/HSS can trigger an update of the allowed CSG list on the UE (based on OMA DM or OTA). This improves the user experience as it enables the UE to automatically select the CSG cell also in the roaming case (without manual CSG selection).

Editor's Note: How to trigger the CSG List Srv to update the Allowed CSG List in the UE is FFS.

The disadvantage of this solution is that in the roaming case it requires an inter-operator interface to allow the CSG Member Mgmt Srv of the VPLMN to update the allowed CSG list of the roaming subscriber. Since the updates over this new interface have no stringent time constraints, a Web-based management interfaces allowing roaming operators (VPLMNs) to provision CSG membership information to the HPLMN might be sufficient.

6.4.1.2.3 Solution 3: Storage of CSG ID for Roaming CSG Members on the network

To handle Roaming CSG Members we propose a new logical entity in the network that only stores subscription data for users that are roaming called the CSS (CSG Subscriber Server). The CSS performs essentially the same function as the HSS except it is only used for CSG specific subscription data and their related procedures.

The CSS has the following properties

- It stores the CSG subscription data for the Roaming CSG Member in the VPLMN to which the CSG belongs
- It uses a Diameter-based interface to the MME or SGSN. The interface to the MSC/VLR is FFS.
- It supports the same set of procedures as the HSS for managing the CSG subscription data for Roaming CSG Members. For example, the CSS needs to update the MME/SGSN/MSC/VLR as defined for the HSS when a subscriber is added/removed from a CSG.

To perform access control for Roaming CSG Member at CSG cells

- The visited MME, SGSN or MSC/VLR needs to retrieve the CSG subscription data for a Roaming CSG Member from the CSS during the attach procedure or tracking/location/routing area updating procedure as part of the UE's roaming subscription profile. If the MME, SGSN or MSC/VLR contacts the CSS for each roaming subscriber, or if it has means to determine which subscribers that have CSG subscription data in CSS, is FFS. The MME, SGSN or MSC/VLR retrieves the rest of the roaming user's profile from the home network using normal procedures as defined for roaming in Rel-8.

The advantages of this solution are as follows:

- No need for the VPLMN to access the HSS of the HPLMN to retrieve the subscription data for the UE
- Additionally, all CSG subscription data for the HPLMN may be also be stored in the CSS to separate this rather dynamic user profile information from the rest of the information stored in the HSS to protect the HSS and simplify the procedures to support CSGs.

6.4.1.2.4 Solution 4: Storage of CSG ID for Temporary CSG Members and Roaming CSG Members on the network

To avoid excessive load for the HSS to handle temporary CSG memberships, and to allow CSG-subscription information for roaming CSG members to be stored in the VPLMN rather than in the HSS of the HPLMN, it is proposed to introduce a new logical entity in the network that stores CSG-Subscription data for CSG members from CSGs within the network. These members may be home subscribers or inbound roamer. The new logical entity is called CSG Subscription Store (CSS). The CSS is located between the MME (or SGSN or VLR) and the HSS and intercepts S6a/S6d (and Gr) signalling. When the CSS detects that subscription data are sent from the HSS to the MME as part of the Update Location Answer command (ULA) it checks its database to see whether the subscriber in question subscribes to CSG information. If so, the CSS sends this information to the MME, either by extending the intercepted ULA message or by issuing a new Insert Subscriber Data Request command (IDR).

The CSS maintains the current MME address for all home subscribers and incoming roamers (unless the current MME is outside the network). When CSG-subscription data in the CSS are added (or modified), the CSS forwards the added (or modified) data to the current MME.

The advantages of this solution are:

1. No need to impact the MME (or SGSN, or VLR). CSG-Subscription data are received by MME from the CSS as if they were received from the HSS.
2. No need to impact the HPLMN. The HSS in the HPLMN does not need to store CSG-Subscription Data.

3. No extensive load in the HSS caused by temporary short lived memberships.

The drawbacks are:

1. The CSS needs to maintain the current MME (and SGSN and VLR) address for all home subscribers and for all incoming roamer. And the CSS is loaded by all HSS signalling. It should therefore be considered to limit this solution to roaming subscribers only, and to do without advantage 3.

2. The CSS needs to intercept S6a/S6d traffic and MAP Gr traffic.

It is FFS how redundancy is provided for the CSS.

6.4.1.3 Evaluation

7 Conclusions

Annex A: Functional split for HNB access as per TS 25.467 [3]

The UTRAN functions in the HNB are supported by RANAP, whereas the HNB specific functions are supported by Home NodeB Application Protocol (HNBAP) between the HNB and the HNB-GW. The HNB-GW provides concentration function for the control plane and may provide concentration function for the user plane.

This sub-clause defines the functional split between the core network and the UMTS radio access network. The functional split is shown in table A-1 and A-2.

Table A-1: Functional split for UTRAN function in the HNB access

Function	HNB	HNB-GW	CN
RAB management functions:			
RAB establishment, modification and release	X	FFS	X
RAB characteristics mapping Iu transmission bearers	X	X	
RAB characteristics mapping Uu bearers	X		
RAB queuing, pre-emption and priority	X		X
Radio Resource Management functions:			
Radio Resource admission control	X		
Broadcast Information	X		X
Iu link Management functions:			
Iu signalling link management	X	X	X
ATM VC management		X	X
AAL2 establish and release		X	X
AAL5 management		X	X
GTP-U Tunnels management	X	X	X
TCP Management	X (FFS)	(X) (Note 1)	X
Buffer Management	X	X	
Iu U-plane (RNL) Management:			
Iu U-plane frame protocol management			X
Iu U-plane frame protocol initialization	X		
Mobility management functions:			
Location information reporting	X		X
Handover and Relocation			
Inter RNC hard HO, Iur not used or not available	X	FFS (Note 4)	X
Serving RNS Relocation (intra/inter MSC)	X (FFS)		X
Inter system hard HO (UMTS-GSM)	X	FFS (Note 4)	X
Inter system Change (UMTS-GSM)	X	FFS	X
Paging Triggering	X		X
GERAN System Information Retrieval	X		X

Function	HNB	HNB-GW	CN
Security Functions:			
Data confidentiality			
Radio interface ciphering	X		
Ciphering key management			X
User identity confidentiality	X		X
Data integrity			
Integrity checking	X		
Integrity key management			X
Service and Network Access functions:			
CN Signalling data	X		X
Data Volume Reporting	X		
UE Tracing	X		X
Location reporting	X	FFS (Note 3)	X
Iu Co-ordination functions:			
Paging co-ordination	X		X
NAS Node Selection Function		X	
MOCN Rerouting Function	FFS	X	X
HNB Registration (Note 2)			
HNB Registration Function	X	X	
HNB-GW Discovery Function	X		
HNB de-registration Function	X	X	
UE Registration for HNB Note 2			
UE Registration Function for HNB	X	X	
UE de-registration Function for HNB	X	X	
Iuh user-plane Management functions			
Iuh User plane transport bearer handling	X	X	

NOTE 1: If TCP is terminated for Iu-BC in the HNB-GW.
NOTE 2: Protocol support for this group of functions is provided by the HNB Application Protocol.
NOTE 3: Whether it is possible (and may be necessary) to provide location information from the HNB-GW (e.g. GW may have logic to derive location based on the public IP address of the HNB-GW, etc). is FFS.
NOTE 4: Support for relocation from the macro network to HNB is FFS.

Editor's note: Functional description of the functions is needed.

Table A-2: Functional split for HNB function in the HNB access

Function	HNB	HNB-GW
HNB Registration (Note 1)		
HNB Registration Function	X	X
HNB-GW Discovery Function	X	
HNB de-registration Function	X	X
UE Registration for HNB (Note 1)		
UE Registration Function for HNB	X	X
UE de-registration Function for HNB	X	X
Iuh user-plane Management functions		
Iuh User plane transport bearer handling	X	X

NOTE 1: Protocol support for this group of functions is provided by the HNB Application Protocol.

Annex B:
Functional split for HeNB access as per TS 36.300 [4]

The HeNB hosts the same functions as an eNB as described in TS 36.300 [4] section 4.1, with the following additional specifications in case of connection to the HeNB-GW:

- Discovery of a suitable Serving HeNB-GW
- A HeNB shall only connect to a single HeNB-GW at one time, namely no S1 Flex function shall be used at the HeNB in case of connection to the HeNB-GW.
    - If the HeNB is connected to a HeNB-GW, it will not simultaneously connect to another HeNB-GW, or another MME.
- The TAC and PLMN ID used by the HeNB shall also be supported by the HeNB-GW.
- When the HeNB connects to a HeNB-GW, selection of an MME at UE attachment is hosted by the HeNB-GW instead of the HeNB.
- HeNBs may be deployed without network planning. A HeNB may be moved from one geographical area to another and therefore it may need to connect to different HeNB-GWs depending on its location.

The HeNB-GW hosts the following functions:

- Relaying UE-associated S1 application part messages between the MME serving the UE and the HeNB serving the UE.
- Terminating non-UE associated S1 application part procedures towards the HeNB and towards the MME. Note that when a HeNB-GW is deployed, non-UE associated procedures shall be run between HeNBs and the HeNB-GW and between the HeNB-GW and the MME.
- Optionally terminating S1-U interface with the HeNB and with the SGW.
- Supporting TAC and PLMN ID used by the HeNB.

In addition to functions specified in TS 36.300 [4] section 4.1, the MME hosts the following functions:

- Access control for UEs that are members of Closed Subscriber Groups (CSG).

Mechanisms for filtering of paging messages, in order to avoid paging message distribution to HeNBs belonging to CSGs where the UE is not registered, is FFS.

Annex C: Actions of MME/SGSN/MSC/VLR upon Allowed CSG List update

The actions of MME/SGSN/MSC/VLR upon Allowed CSG List update are summarized in the following table. Please refer to clause 6.1.4, clause 6.3.2, clause 6.3.4 and clause 6.3.7 for more details.

Table C-1: MME/SGSN/MSC/VLR actions upon ACL update

UE state	Change to the ACL	Current camping cell	Access mode	Actions of MME/SGSN/MSC/VLR
ECM-CONNECTED/ READY	Add a CSG ID	CSG cell of this CSG	Hybrid	MME/SGSN/MSC/VLR stores the updated Allowed CSG List and informs the membership change of the UE (i.e. the membership is changed from non CSG member to CSG member) to H(e)NB. (NOTE 3)
		Other cell (NOTE 1)	/ (NOTE 2)	MME/SGSN/MSC/VLR just stores the updated Allowed CSG List, no other action is performed.
	Remove a CSG ID or a CSG ID is expired	CSG cell of this CSG	Hybrid	MME/SGSN/MSC/VLR stores the updated Allowed CSG List and informs the membership change of the UE (i.e. the membership is changed from CSG member to non CSG member) to H(e)NB. (NOTE 3)
			Closed	Which solution described below should be chosen is FFS: 1) The MME/SGSN/MSC/VLR indicates to the H(e)NB that the UE is no longer permitted to access the CSG. By receiving the indication, the H(e)NB tries to handover the UE to a suitable cell. 2) The MME/SGSN/MSC/VLR performs S1/Iu release procedure with appropriate cause. (NOTE 4)
		Other cell (NOTE 1)	/ (NOTE 2)	MME/SGSN/MSC/VLR just stores the updated Allowed CSG List, no other action is performed.
	Expiration date is extended.	CSG cell of this CSG	Hybrid	
			Closed	
		Other cell (NOTE 1)	/ (NOTE 2)	
ECM-IDLE/ STANDBY	All cases			
NOTE 1: "Other cell" may be a macro cell, an open cell, or a CSG cell belongs to other CSG ID. NOTE 2: "/" includes all cases including macro, open, hybrid and closed. NOTE 3: This is according to clause 6.3.4.2.2 that "*In case of changes of the CSG membership status (e.g. expiry of temporary CSG membership), it should be possible for the Core Network node to convey this change to the H(e)NB dynamically*.", which allows admission control and rate control for hybrid access mode as required by SA WG1. NOTE 4: See clause 6.3.2 for evaluation.				

Annex D:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2009-09	SA#45	SP-090611	-	-	MCC editorial update to version 1.0.0 for presentation to TSG SA for information and approval	0.6.0	1.0.0
2009-09	SA#45	MCC	-	-	MCC update to version 9.0.0 after approval at TSG SA#45	1.0.0	9.0.0