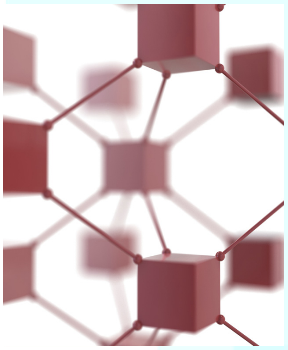

3GPP Femtocells: Architecture and Protocols

by Gavin Horn

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-1714
U.S.A.

3GPP Femtocells: Architecture and Protocols
September 2010

Contents

Figures

Foreword

This document defines the functionalities for the support of Home NodeBs (HNB) and Home eNodeBs (HeNB) – jointly referred to as H(e)NB – including the functionalities to support Closed Subscriber Groups (CSG) as currently defined in 3GPP. It is intended as a one stop guide to provide an overview of the current status of the standards for operators and manufacturers interested in the deployment of H(e)NBs including references to where more details on each subject can be found.

The contents of the document include the following:

- Description of the existing procedures relating to H(e)NBs specified for Rel-9.
- Discussion of some details relating to H(e)NBs which may be considered out of scope of the 3GPP standards but are needed to achieve a successful H(e)NB deployment.

1. Scope

The following procedures need to be addressed to enable the successfull deployment of H(e)NBs:

1. CSG provisioning
   - Provisioning a subscriber at a CSG
   - Management of the CSG subscription data in the network
   - Management of the CSG subscription data at the UE
   - Management of conflicts for the CSG subscription data between the network and the UE
2. Access Control
   - Procedures for access control when establishing the connection at a CSG cell or a hybrid cell
   - Procedures for access control for in-bound handover to a CSG cell or a hybrid cell
   - Differentiating between a CSG member and a non-CSG member at a hybrid cell
3. Mobility management
   - Idle mode procedures for a CSG cell or a hybrid cell
   - Connected mode procedures for a CSG cell or a hybrid cell
   - Paging and registration at CSG cells
4. IMS Emergency Session Support
5. Security procedures for the H(e)NB
6. OAM procedures for the H(e)NB
7. Differentiated CSG charging

2. References

[1] 3GPP TS 23.060, "General Packet Radio Service (GPRS); Service description; Stage 2".

[2] 3GPP TS 23.401, "GPRS enhancements for E-UTRAN access".

[3] 3GPP TS 36.304, "E-UTRA UE procedures in idle mode".

[4] 3GPP TS 25.304, "UE procedures in idle mode and procedures for cell reselection in connected mode".

[5] 3GPP TS 23.122, "NAS functions related to MS in idle mode".

[6] 3GPP TS 22.011, "Service accessibility".

[7] 3GPP TS 36.300, "E-UTRA and E-UTRAN; Overall description; Stage 2".

[8] 3GPP TS 22.220, "Service requirements for Home NodeBs and Home eNodeBs".

[9] 3GPP TS 31.102, "Characteristics of the USIM application".

[10] 3GPP TS 33.320, "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[11] OMA-ERELD-DM-V1_2, "Enabler Release Definition for OMA Device Management".

[12] OMA-TS-DM_Protocol-V1_2, "OMA Device Management Protocol, Version 1.2".

[13] OMA-TS-DM_Notification-V1_2, "OMA Device Management Notification Initiated Session, Version 1.2".

[14] 3GPP TS 25.467, "UTRAN architecture for 3G Home NodeB".

[15] 3GPP TS 36.413, "S1 Application Protocol".

[16] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".

[17] 3GPP TS 24.008, "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[18] 3GPP TS 31.111, "USIM Application Toolkit (USAT)".

[19] 3GPP TS 23.012, "Location Management Procedures".

[20] 3GPP TS 23.002, "Network architecture".

[21] IETF RFC 3588, "Diameter Base Protocol".

[22] 3GPP TS 23.008, "Organization of subscriber data".

[23] 3GPP TS 36.423, "X2 Application Protocol".

[24] 3GPP TS 32.581, "Concepts and Requirements for Type 1 interface HNB to HNB Management System (HMS)"

[25] 3GPP TS 32.582, "HNB OAM&P; Information model for Type 1 interface HNB to HNB Management System (HMS)".

[26] Broadband Forum TR-069 Amendment 2, "CPE WAN Management Protocol v1.1".

[27] Broadband Forum TR-196, "Femto Access Point Service Data Model".

[28] 3GPP TS 24.285, "Allowed Closed Subscriber Group (CSG) List Management Object (MO)".

[29] 3GPP TS 29.002, "Mobile Application Part (MAP) specification".

[30] 3GPP TS 29.272, "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

[31] 3GPP TS 23.003, "Numbering, addressing and identification".

[32] 3GPP TS 25.413, "UTRAN Iu interface; Radio Access Network Application Part (RANAP) signalling".

[33] 3GPP TS 25.331, "Radio Resource Control (RRC)."

[34] 3GPP TS 36.331, "E-UTRA Radio Resource Control (RRC)."

[35] 3GPP TS 25.133, "Requirements for support of radio resource management."

[36] 3GPP TS 36.133, "Requirements for support of radio resource management."

[37] 3GPP TS 33.210, "3G security; Network Domain Security (NDS); IP network layer security".

[38] Open Mobile Alliance OMA-WAP-OCSP V1.0: "Online Certificate Status Protocol Mobile Profile". URL: http://www.openmobilealliance.org/

[39] IETF RFC 4806, "Online Certificate Status Protocol (OCSP) Extensions to IKEv2".

[40] IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[41] 3GPP TS 32.583, "Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure Flows for Type 1 Interface HNB to HNB Management System".

[42] 3GPP TS 32.593, "Telecommunications management; Home eNodeB B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure Flows for Type 1 Interface HeNB to HeNB Management System ".

[43] 3GPP TS 23.203, "Policy and charging control architecture".

[44] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3. Definitions and abbreviations

For the purposes of the present document, the following terms and definitions below apply. Terms and definitions not defined below can be found in TR 21.905 [44].

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 manager: A CSG manager can, under the operator's supervision, add, remove and view the list of CSG members.

CSG subscription data: A list of CSG IDs stored in the network containing the CSG identities of the CSGs to which the subscriber belongs. A UE is able to access only those CSG cells that have a CSG ID in this list.

NOTE: The CSG subscription data may be temporarily out of sync with the CSG Whitelist when a UE is added or removed from a CSG or the CSG membership expires.

Allowed CSG list: A list stored in the UE, under both user and operator control, containing the CSG identities and associated PLMN identities of the CSGs to which the subscriber belongs.

Operator CSG list: A list stored in the UE, under exclusive operator control, containing the CSG identities and associated PLMN identities of the CSGs to which the subscriber belongs.

CSG Whitelist: The union of the Allowed CSG list and Operator CSG list, provided by NAS to AS.

HNB: A customer premises equipment that connects a 3GPP UE over UTRAN wireless air interface and to an operator’s network using a broadband IP backhaul.

HeNB: Customer-premises equipment that connects a 3GPP UE over E-UTRAN wireless air interface and to an operator’s network using a broadband IP backhaul.

HNB subsystem: The Home NodeB Subsystem (HNS) consists of a Home NodeB (HNB) and Home NodeB Gateway (HNB-GW). The Home NodeB Subsystem appears as an RNS to the core network and is connected by means of the Iu-CS interface to the MSC and by means of the Iu-PS interface to the SGSN.

HeNB subsystem: The Home eNodeB Subsystem (HeNS) consists of a Home eNodeB (HeNB) and optionally a Home eNodeB Gateway (HeNB-GW). The Home eNodeB Subsystem is connected by means of the S1 interface to the EPC (Evolved Packet Core), more specifically to the MME (Mobility Management Entity) by means of the S1-MME interface and to the Serving Gateway (S-GW) by means of the S1-U interface.

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

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

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

H(e)NB Hosting Party: A Hosting Party has a contractual relationship with the operator, related to one or more H(e)NBs.

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

4. Architecture model and functions

4.1. Architecture reference model

4.1.1.Home NodeB Subsystem architecture reference model

The Home NodeB Subsystem (HNS) consists of a Home NodeB (HNB) and Home NodeB Gateway (HNB-GW). The Home NodeB Subsystem appears as an RNS to the core network and is connected by means of the Iu-CS interface to the MSC and by means of the Iu-PS interface to the SGSN.

Figure 4-1 describes the HNB architecture including the CSG provisioning elements.

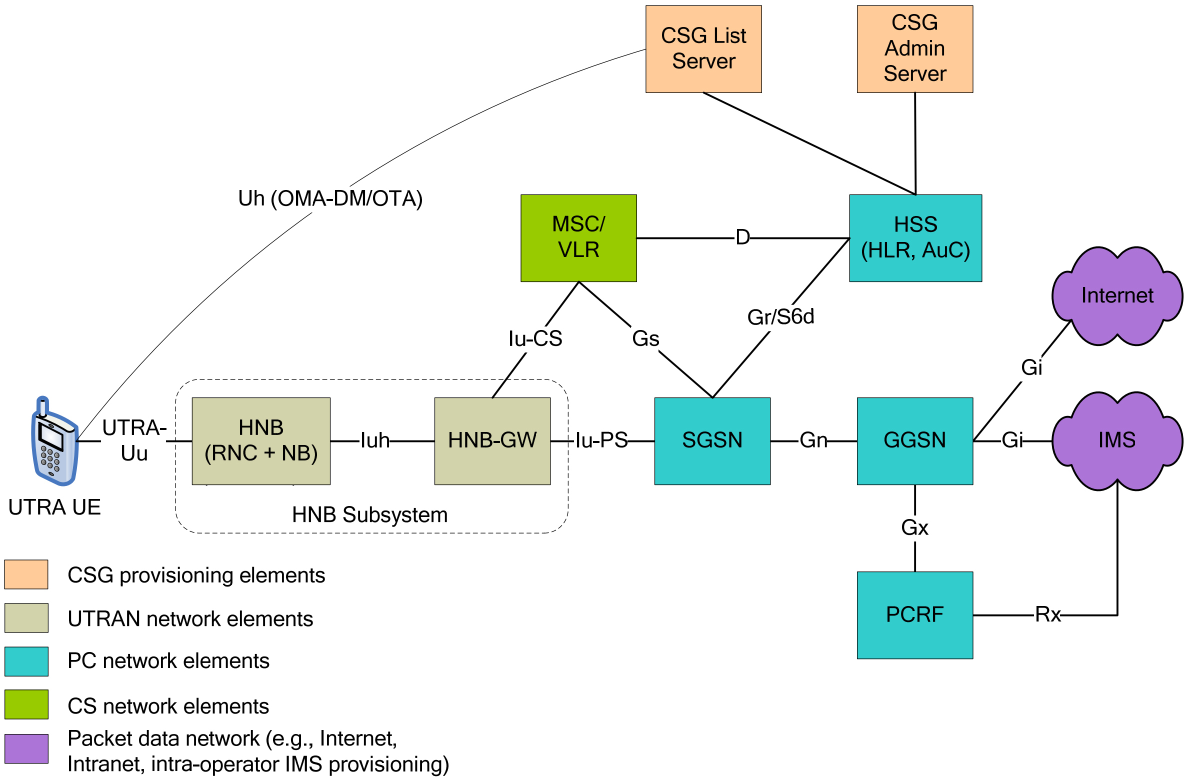

Figure 4-1: UTRAN network architecture for CSG provisioning and access control

NOTE: Additional interfaces for 2G/3G access are shown in TS 23.002 [20].

The UTRAN network elements include:

- The Home NodeB (HNB) is a Customer Premises Equipment (CPE) which includes the UTRAN NodeB offering UTRAN coverage and most of the UTRAN RNC functions as well as new functions to support HNB authentication, HNB-GW discovery, HNB registration and configuration through OAM, optional UE access control and UE registration at HNB-GW. Further details can be found in TS 25.467 [14].

- The Home NodeB Gateway (HNB-GW) is the gateway through which the Home NodeB accesses the core network and includes the HNB and UE registration functions, UE access control, and an Iu handling function to connect the HNB to the core network. Some optimization functions such as paging optimization for the UEs under HNB coverage may also be included. Further details can be found in TS 25.467 [14].

NOTE: The HNB authentication function resides in the Security Gateway (not shown) which may or may not be collocated with the HNB-GW. Further details can be found in Section 9.

NOTE: The OAM functions for the HNB are not shown. The HNB uses a TR-069 interface to the OAM function to push or receive configuration parameters. Further details can be found in Section 10.

The PC network elements and the packet data network are the same as already defined in TS 23.060 [1].

The CS network elements and the circuit switched network are the same as already defined in TS 23.060 [1].

The CSG provisioning network elements include:

- The CSG List Server hosts functions used by the subscriber to manage membership to different CSGs. For example, the CSG List Server includes the UE CSG provisioning functions which manage the Allowed CSG List and the Operator CSG list stored on the UE.
- The CSG Administration Server hosts functions used by the CSG manager to manage the CSG. For example, the CSG Administration Server includes the CSG administration function which manages the list of subscribers for a CSG, i.e., the access control list for the CSG.

NOTE: The interfaces to the HLR for the CSG Administration Server and CSG List Server are not specified in the standard. The interface to the CSG Administration Server provides a similar functionality to the interface that exists to the HSS today that is used to manage other user subscription data, for example as subscribers join or leave an operator’s network.

NOTE: The CSG Administration Server and CSG List Server are common for UTRAN and E-UTRAN to support CSGs with a single CSG ID that include both HNBs and HeNBs.

4.1.2. Home eNodeB Subsystem architecture reference model

The Home eNodeB Subsystem (HeNS) consists of a Home eNodeB (HeNB) and optionally a Home eNodeB Gateway (HeNB-GW). The Home eNodeB Subsystem is connected by means of the S1 interface to the EPC (Evolved Packet Core), more specifically to the MME (Mobility

Management Entity) by means of the S1-MME interface and to the Serving Gateway (S-GW) by means of the S1-U interface.

Figure 4-2 describes the HeNB architecture including the CSG provisioning elements.

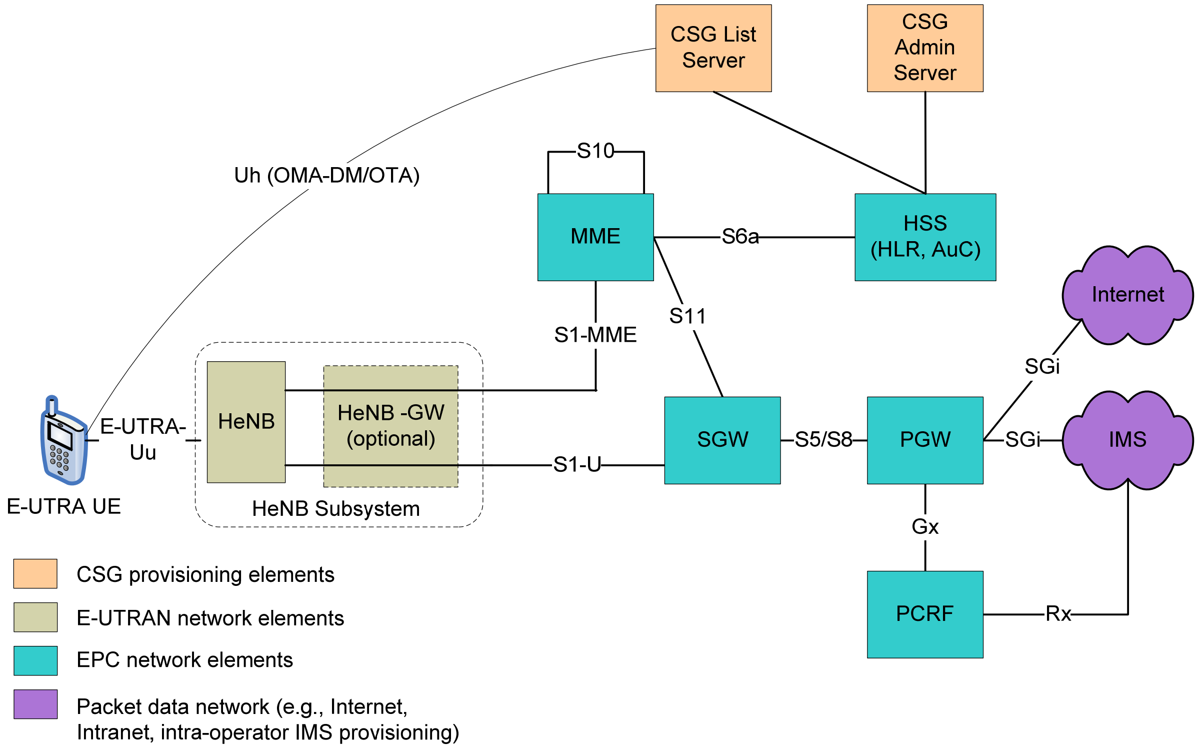

Figure 4-2: E-UTRAN network architecture for CSG provisioning and access control

The E-UTRAN network elements include:

- The Home eNodeB (HeNB)) is a Customer Premises Equipment (CPE) which includes the E-UTRAN eNodeB offering E-UTRAN coverage as well as new functions to support HeNB authentication, HeNB registration and configuration through OAM. Further details can be found in TS 36.300 [7].
- The Home eNodeB Gateway (HeNB-GW) is an optional gateway through which the Home eNodeB accesses the core network. The Home eNodeB Gateway may also be used only for the S1-MME interface. In this case, the S1-U interface is directly between the Home eNodeB and the S-GW. Some optimization functions such as paging optimization for the UEs under HeNB coverage may also be included. Further details can be found in TS 36.300 [7].

NOTE: The HeNB authentication function resides in the Security Gateway (not shown) which is a separate logical entity which may or may not be collocated with the HeNB GW if present. The HeNB and HNB authentication functions are common. Further details can be found in Section 9.

NOTE: The HeNB configuration functions are common to the configuration functions for HNB. The OAM functions for the HeNB are not shown. Further details can be found in Section 10.

The EPC network elements and the packet data network are the same as already defined in TS 23.401 [2].

The CSG provisioning network elements are common for UTRAN and E-UTRAN and are defined in Section 4.1.1.

4.2. High level functions

The following list gives the logical network protocol functions to support CSG cells:

- CSG provisioning functions
- Access control functions
- Mobility management functions
- IMS Emergency Session Support functions
- Security functions
- OAM functions

4.2.1.CSG provisioning functions

The CSG provisioning function performs two roles

- Managing the list of subscribers for a CSG.
  - This function may be hosted by the operator or a third party.
  - A single list manages all the HNBs and HeNBs for a CSG, i.e. all HNBs and HeNBs advertising the same CSG identity in the same PLMN will have a single list of subscribers.
- Managing how the CSG information is stored in the UE and the network.
  - Provisioning of the Allowed CSG list and the Operator CSG list on the UE in order to avoid accessing non-allowed CSG cells; and
  - Storage of the CSG subscription information in the network in order to perform access control.

Further details of the CSG provisioning functions can be found in Section 5.

4.2.2. Access control functions

The access control functions ensure a UE has a valid subscription at a CSG cell where it performs an access or a handover. The access control indicates whether the UE is a member or non-member with the associated CSG ID when accessing a hybrid cell.

Further details of the access control functions can be found in Section 6.

4.2.3. Mobility management functions

The mobility management functions are used to keep track of the current location of a UE.

Further details of the access control functions can be found in Section 7.

4.2.4. IMS Emergency Session Support functions

The IMS Emergency Session Support functions are described in Section 8.

4.2.5. Security functions

The security functions are described in Section 9.

4.2.6. OAM functions

The OAM functions are described in Section 10.

5. CSG provisioning

5.1. General

CSG provisioning includes adding or deleting a subscriber from the CSG list of subscribers as well as viewing the list of subscribers.

There are four aspects to be considered to support CSG provisioning:

- Provisioning a subscriber at a CSG, i.e., how the subscriber is added or removed from the list of subscribers for a CSG.
- Management of the CSG subscription data in the network, i.e., how the CSG subscription data for a subscriber is stored in the network.
- Management of the CSG subscription data at the UE, i.e., how the Allowed CSG list and the Operator CSG list are updated at the UE.
- Management of out-of-date CSG information at the UE by the network, i.e., how to manage any delays between when the CSG subscription data is updated on the network and when it is updated at the UE.

5.2. Provisioning a subscriber at a CSG

5.2.1.Requirements for provisioning CSG membership

According to TS 22.220 [8], the CSG manager is allowed to add, remove and view CSG membership as well as to set a time limit for temporary members of a CSG.

In particular, TS 22.220 [8] defines the following requirements for managing CSG membership:

- The CSG manager shall be able, under the operator supervision, to add, remove and view CSG membership.
- For temporary members, it shall be possible to limit the period of time during which the subscriber is considered a member of a CSG (granted access rights). It shall be possible to configure a time period for each temporary member.
- The time period shall be configurable by the CSG manager and/or the operator operating the CSG cell and shall span from 1 deci-hour to several days. Unlimited membership to the CSG is allowed.
- When the time period expires, the CSG shall no longer be considered to be available to provide services, except for emergency calls and it shall be possible for established communication via a CSG cell to be diverted from the CSG cell.

NOTE: Provisioning a subscriber at a CSG applies to both CSG cells and hybrid cells.

5.2.2. Provisioning a subscriber by the CSG Administration Server

The CSG Administration Server hosts the functions for provisioning a subscriber at a CSG by providing a user interface to the CSG manager and possibly the subscriber.

Provisioning a subscriber at a CSG may be initiated by the CSG manager or the subscriber.

Choices for the user interface to the CSG Administration Server include:

- A HTTP-based interface (e.g. a CSG menu tab included in the web page the CSG manager may already use to control other aspects of their account such as billing).
- A UE-based application (e.g., an application on the UE used by the CSG manager similar to the one that manages a contact list or an address book).
- A command line interface (e.g., for enterprise deployments that run an automated script to add or removed employees).

NOTE: The CSG Administration Server is outside the scope of 3GPP standardization.

The CSG Administration Server updates the CSG subscription data stored in the network by the HSS/HLR when a subscriber is added to or removed from a CSG. Further details can be found in Section 5.6.

5.3. Management of the CSG subscription data in the network

Figure 5-1 shows how the CSG subscription data is stored in the network when the UE is attached in the HPLMN.

The CSG subscription data is stored in the HSS/HLR as part of the subscriber data as specified in TS 23.060 [1] and TS 23.401 [2]. The CSG subscription data is defined as a list of up to 50 CSG-Ids per PLMN and for each CSG-Id an optional associated expiration date which indicates the time when the subscription to the CSG-Id expires; an absent expiration date indicates unlimited subscription. The structure of the CSG related parameters are defined in TS 23.003 [31].

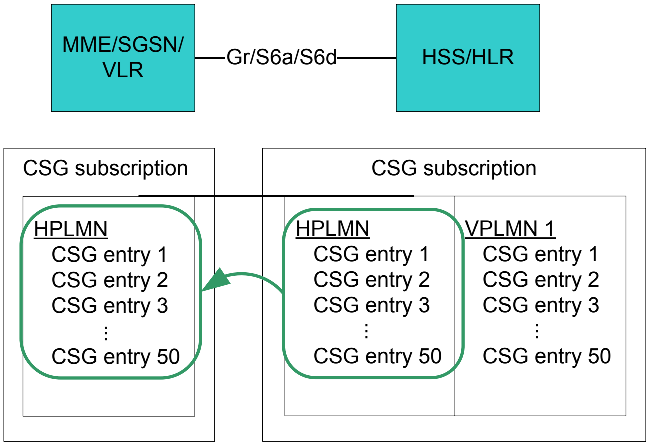

Figure 5-1: Network storage of the CSG subscription data

The CSG subscription information is transferred to the MME/SGSN/MSC/VLR using the MAP (TS 29.002 [29]) or Diameter (TS 29.272 [30]) protocols as follows:

- The CSG subscription data for the registered PLMN is forwarded to the MME/SGSN/MSC/VLR serving the UE during the attach procedure and whenever the MME/SGSN/MSC/VLR serving the UE changes.
- The applicable CSG subscription data is forwarded to the MME/SGSN/MSC/VLR when the CSG subscription information for the current registered PLMN changes. For example, if a subscriber is added to or removed from a CSG, or an expiration date is changed.
- The CSG subscription data in the MME/SGSN/MSC/VLR is not updated because of expiry of a CSG membership.

NOTE: This is an optimization to reduce the amount of signalling needed between the HSS/HLR and the MME/SGSN/MSC/VLR.

For UTRAN, the access control list, i.e., the list of IMSIs of all the subscribers for a CSG, is also stored in an OAM function and pushed to or retrieved by the HNB-GW. For example, the CSG Administration Server may have an interface to the OAM function to update the access control list when a subscriber is added or removed.

If the HNB performs access control, the access control list is also pushed to or retrieved by the HNB by the OAM function using the TR-069 interface.

NOTE: The most efficient method to store the access control list in the HNB GW or OAM is per CSG as opposed to per HNB, for example for an enterprise with many HNBs in the CSG only one list is needed for the CSG.

5.4. Management of the CSG subscription data at the UE

5.4.1. General

TS 22.220 [8] defines the following requirements related to management of the CSG subscription data at the UE:

- The UE shall contain a list of allowed CSG identities (Allowed CSG List). It shall be possible to store the Allowed CSG List in the USIM. When available, the list on the USIM shall be used. It shall be possible for both, the operator and the UE, to modify the Allowed CSG List.
- The UE shall allow the user to introduce new CSGs to the Allowed CSG List by means of manual CSG selection only.
- The UE shall maintain an operator controlled list of allowed CSG identities (Operator CSG list). It shall be possible to store the Operator CSG list in the USIM. When available, the list on the USIM shall be used. It shall be possible for the operator to modify the Operator CSG List.
- The two lists are maintained independently from each other. A change in the Operator CSG list shall not trigger the UE to modify the Allowed CSG list to reflect such change automatically.
- All CSG cells belonging to a CSG identity not included in the Allowed CSG List or Operator CSG list shall be considered not suitable by the UE ("not suitable" as specified in TS 25.304 [4] and TS 36.304 [3]).

NOTE: The reason for defining the Operator CSG list is to mandate a list that can only be updated by the operator, i.e., the Operator CSG list is read-only and cannot be modified by the user.

NOTE: CSG subscription data at the UE is only applicable to Rel-8 UEs and onwards and is applicable to both CSG and hybrid cells at both HNBs and HeNBs.

5.4.2. Provisioning a CSG in the UE's Allowed CSG list

The Allowed CSG list is read/write by the UE and provisioned using OMA DM, OTA or NAS procedures. There are two agreed mechanisms to update the Allowed CSG list at the UE:

- **Application level update:** using the OTA procedures for a UE with a Rel-8 USIM as defined in TS 31.102 [9] and OMA DM procedures for a UE with a pre-Rel-8 USIM as defined in TS 24.285 [11].
  - The OMA DM or OTA procedures are used to add or remove one or more CSG IDs in the Allowed CSG list. Further details of the OMA DM procedures can be found in Section 5.4.2.1.

- **Manual update:** using the NAS procedures. The UE updates the Allowed CSG list according to the response to the Attach, Location Registration (LAU/RAU/TAU), Detach and Service Request procedures.
    - At any time, the user can trigger the UE to search for and access neighbouring CSG cells using manual CSG selection. If the user selects a CSG which is not present in the Allowed CSG list or the Operator CSG list, then the UE will perform a Location Registration procedure at the selected CSG cell. If the Location Registration procedure is successful, then the UE adds the CSG ID to the Allowed CSG list if not already present. Further details can be found in Section 5.4.2.2.
    - If the permissions for a UE to access a H(e)NB are removed and have not been updated via an Application level update, then when the UE performs an Attach, Detach, Service Request or Location Registration procedure, the MME/SGSN/MSC will reject the UE with reject code #25 (Not authorized for this CSG) and the CSG ID will be removed from the Allowed CSG list if present.

NOTE: If the membership in the CSG is withdrawn while the UE is in connected mode at the CSG, the network performs an S1/Iu release of the UE. The CSG entry is not removed from the Allowed CSG list by this procedure.

5.4.2.1. Application level update using OMA DM

In addition to the OTA procedures defined in TS 31.111 [18] for provisioning a UE with a Rel-8 USIM, OMA DM procedures have been defined for provisioning a UE with a pre-Rel-8 USIM. The information elements (IEs) provisioned by OTA and OMA DM are common.

The Allowed CSG Management Object defined by OMA DM has the following elements TS 24.285 [28]:

- PLMN Identifier (or PLMN ID)
    - CSG Identifier (or CSG ID)
    - Home NodeB Name (or HNB Name)
    - CSG Type

The structure of the above OMA DM CSG related parameters is defined in TS 23.003 [31].

The OMA Device Management (OMA DM) [11] protocol enables distribution of any kind of information such as applications, data and configuration settings to any single handset or groups of handsets.

The protocol allows two-way communication and is used for data exchange between the OMA DM Server (which is managing the device) and the OMA DM client. The communication protocol is a request-response protocol and supports a push as well as a pull model. It is assumed here that the UE contains an OMA DM client, and that the CSG List Server contains an OMA DM server.

OMA Device Management consists of two stages:

- **Bootstrap:** the process of provisioning the OMA DM client to a state where it is able to initiate a management session to a new OMA DM server.
- **DM Provisioning:** the process by which an OMA DM server provisions the device with further information after the device is bootstrapped.

In the bootstrap process a trust relationship is created between the OMA DM client and the OMA DM server. There is only one bootstrap needed per OMA DM server and OMA DM client pair.

Once the bootstrap process has been carried out, the OMA DM client in the UE and the OMA DM server in the CSG List Server may start to communicate using the OMA DM provisioning process.

Either the UE or CSG List Server may initiate the provisioning of information. A typical message flow is shown in Figure 5-2.

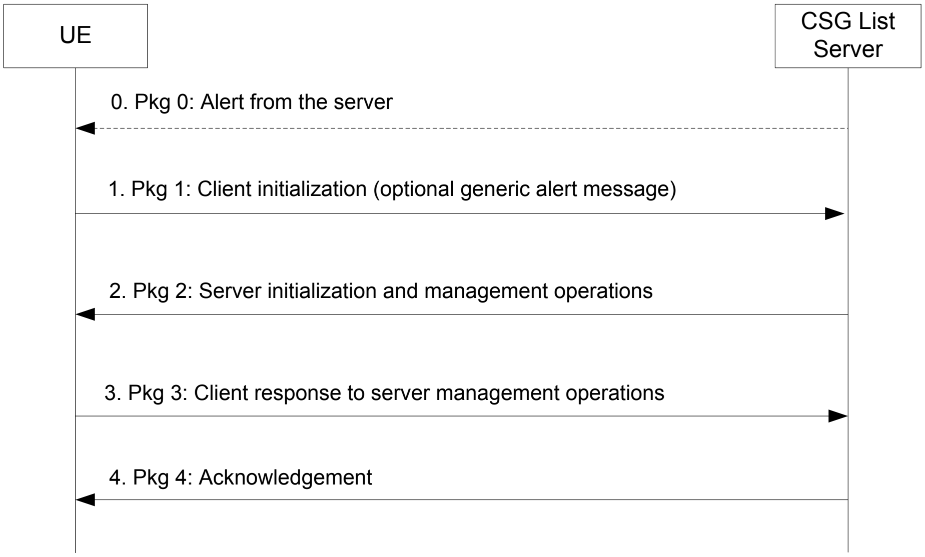
UE
CSG List Server
0. Pkg 0: Alert from the server
1. Pkg 1: Client initialization (optional generic alert message)
2. Pkg 2: Server initialization and management operations
3. Pkg 3: Client response to server management operations
4. Pkg 4: Acknowledgement

Figure 5-2: OMA DM CSG provisioning of information

0. When the CSG List Server initiates the provision of information, it sends an OMA DM package 0 notification containing a session alert message to cause the UE to initiate a connection back to the CSG List Server.
1. The UE sends OMA DM package 1 containing: device information (like manufacturer, model etc), client identification.
   - In the case the UE initiated the provisioning of information, package 1 contains an indication of client initiated session, and a Generic Alert message.

  - In the case the CSG List Server initiated the provisioning of information package 1 contains an indication of a server initiated session.

2. The CSG List Server sends OMA DM package 2 containing: server identification, and management data and commands to update the Allowed CSG list and the Operator CSG list in the UE.
3. The UE sends OMA DM package 3 containing results of the management actions sent from server to client.
4. The CSG List Server sends OMA DM package 4 to close the management session.

The detailed contents and coding of the different packages are described in OMA-TS-DM_Protocol-V1_2 [12] and OMA-TS-DM_Notification-V1_2 [13].

5.4.2.2. Manual update using Manual CSG selection

The following behaviour is defined for manual CSG selection:

- The user may select a CSG in any PLMN according to the requirements defined in TS 22.220 [8].

If the user selects a CSG cell within the same PLMN it is currently camped on, there is no interaction between PLMN selection and manual CSG selection. In this case, if the user selects a CSG whose CSG identity is not included in the Allowed CSG list or Operator CSG list, then the UE shall attempt to register on a cell that corresponds to the CSG.

However, if the user selects a CSG cell in a different PLMN than the one it is currently camped on, then TS 22.220 [8] defines the following requirements:

- When the user manually selects a CSG identity in a PLMN, which is different from the last registered PLMN, the following behaviour applies:
  - The UE shall enter into Manual PLMN Selection state.
  - The UE shall attempt to register to the PLMN. This PLMN shall not be stored as the Last Registered PLMN.
  - When the UE is no longer in the service area of the CSG cell the UE shall return to the previous PLMN Selection state.

Manual CSG selection applies to both CSG cells and hybrid cells. If the UE registers in response to manual CSG selection via a hybrid cell, the network does not perform access control. Because of this, the UE is not aware if it has been admitted to the hybrid cell as a CSG member or non-member and so the UE does not add the corresponding CSG ID to its Allowed CSG List.

NOTE: Adding a CSG ID to the UE's Allowed CSG List for a hybrid cell is performed only by OTA or OMA DM procedures.

An example call flow between the NAS and the AS in a UE for manual CSG selection across PLMNs is shown in Figure 5-3.

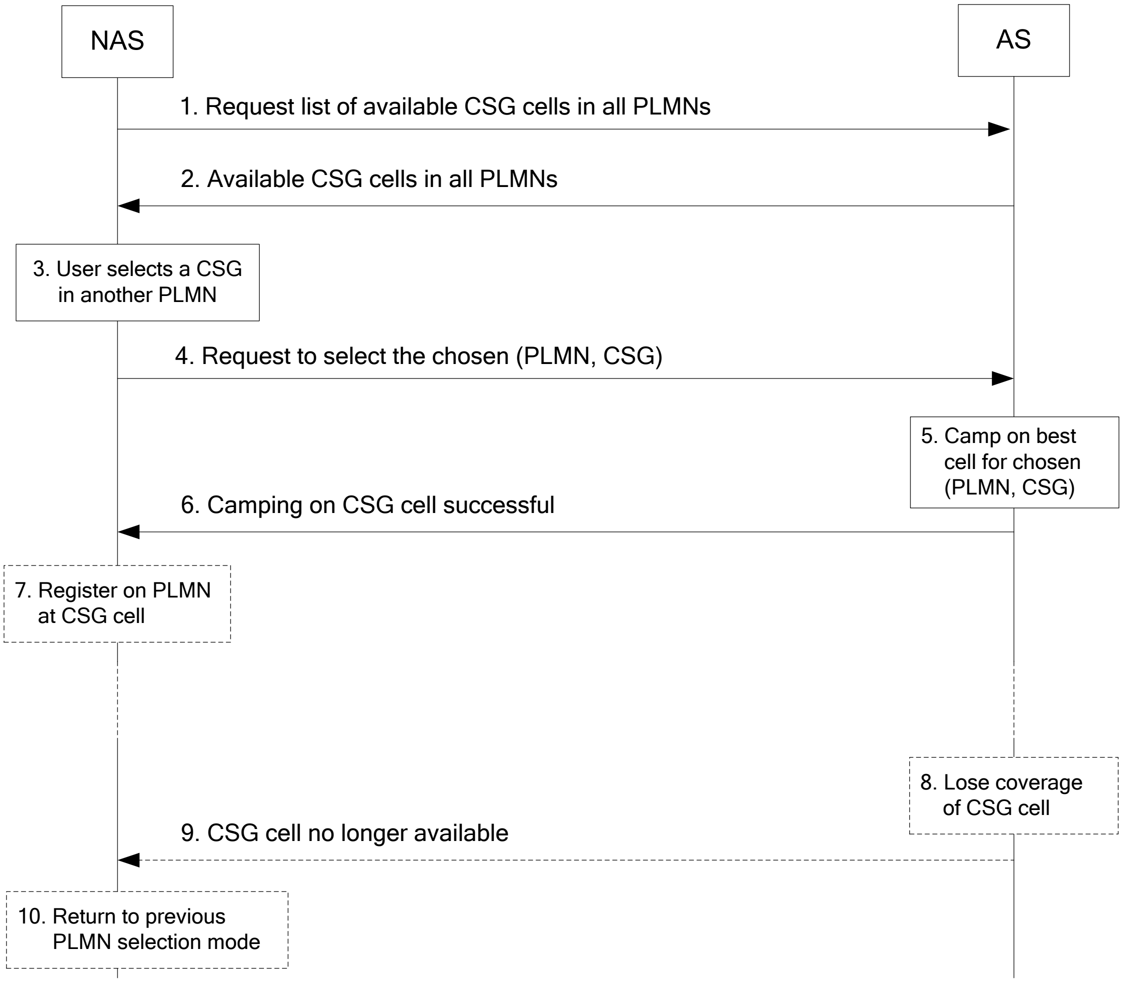
NAS
AS
1. Request list of available CSG cells in all PLMNs
2. Available CSG cells in all PLMNs
3. User selects a CSG in another PLMN
4. Request to select the chosen (PLMN, CSG)
5. Camp on best cell for chosen (PLMN, CSG)
6. Camping on CSG cell successful
7. Register on PLMN at CSG cell
8. Lose coverage of CSG cell
9. CSG cell no longer available
10. Return to previous PLMN selection mode

Figure 5-3: Example call flow of manual CSG selection between the NAS and the AS in a UE

1. The user requests manual CSG selection which triggers the NAS in the UE to request a list of available CSG cells across all PLMNs. The manual CSG selection applies to CSG cells both in and out of the UE's Allowed CSG list and Operator CSG list.

NOTE: For UMTS, TS 25.304 [4], states that a UE is not required to support manual search and selection of CSG ID(s) while in RRC CONNECTED state.

NOTE: For LTE, TS 36.304 [3] states that a UE is not required to support manual search and selection of PLMN or CSG IDs while in RRC CONNECTED state. The UE may use a local release of RRC connection to perform manual search if it is not possible to perform the search while RRC connected.

2. In response to the NAS request, the AS shall scan all RF channels according to its capabilities and returns a list of available CSG cells for a user to select from across all PLMNs.

    - The UE scans the UTRA and E-UTRA bands according to its capabilities to find available CSG IDs.

    On each carrier, the AS shall at least search for the strongest cell, read its system information and report available CSG ID(s) together with their associated PLMN and HNB name (if available) to the NAS for the user to select from.

    The search for available CSG IDs may be stopped on request of the NAS.

3. The UE displays to the user the CSGs that are available and the associated PLMNs. The HPLMN shall configure, on a PLMN basis, the UE to display the available CSGs so that either:

    - All CSGs are displayed, or
    - Only CSGs in the Operator CSG List are displayed.

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

    The UE should also indicate the text based HNB Name if available. The available CSG IDs shall be displayed in the following order:

    - The CSG IDs that are contained in the Allowed CSG list.
    - The CSG IDs that are contained in the Operator CSG list.
    - Any other CSG ID not included in the Allowed CSG list or Operator CSG list.

    When there are multiple cells with the same CSG ID on the same PLMN, only the HNB Name of the strongest cell for that CSG ID is displayed. The UE may also display other information such as the signal strength of the CSG cell and whether the CSG cell belongs to the current PLMN. For instance, a UE may use signal strength bars to indicate that it has detected the presence of the CSG cell but the UE may not select it due to unsuitable RF conditions. The UE shall not display a PLMN for which there is no CSG cell available for selection.

NOTE: The HNB Name may be stored in the USIM. If the HNB Name stored on the USIM is available, it shall take precedence over the broadcasted HNB Name.

NOTE: The HNB Name may be stored optionally in the ME. If the HNB Name is present in the USIM, the HNB Name in the ME shall be ignored. If the HNB Name is present in the Operator CSG list, a HNB Name present in the Allowed CSG list shall be ignored..

4. The NAS requests the AS to camp on the manually selected (PLMN, CSG) pair.

5. The AS performs the reselection procedures required to camp on the best cell in that PLMN for that CSG by searching for an acceptable or suitable cell belonging to the selected CSG ID as specified in TS 25.304 [4] and TS 36.304 [3].

6. The AS returns an indication that camping on the CSG cell was successful including details of the CSG cell such as CSG ID, TAC/LAC/RAC.

7. If the user selects a CSG cell within the same PLMN it is currently camped on, and the CSG cell has a CSG ID that is not in either the UE's Allowed CSG list or the Operator CSG list, then the UE performs a Location Registration procedure (LAU/RAU/TAU) irrespective of the advertised LAC/RAC/TAC of the CSG cell. If the UE performs a successful Location Registration procedure, then the UE shall add the CSG to the Allowed CSG list if it is not already present.

   If the user selects a CSG cell in a PLMN that is different from the RPLMN, then the following applies:

   i) The UE shall store a duplicate of the RPLMN and a duplicate of the current PLMN selection mode;

   ii) The UE shall enter into Manual mode of PLMN selection in state M4 (Trying PLMN) as defined in clause 4.3.1.2 of TS 23.122 [5];

   iii) The UE shall select the PLMN corresponding to the CSG and attempt to register on the selected CSG cell in the PLMN;

   iv) If the registration fails, then the UE shall return to the stored duplicate PLMN selection mode and use the stored duplicate value of RPLMN and initiate the procedures to reselect to a cell on the appropriate PLMN including registering on the PLMN.

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

8. The UE loses coverage of the CSG or other RF conditions cause the UE to move out of coverage of cell(s) belonging to the selected CSG.

9. The AS informs the NAS that a CSG cell with the same CSG ID is no longer available for reselection.

10. If the user had previously selected a CSG cell in a PLMN that is different from the RPLMN in step 3, then when the UE is no longer in the coverage of the CSG, the UE shall return to the stored duplicate PLMN selection mode and use the stored duplicate value of RPLMN and initiate the procedures to reselect to a cell on the appropriate PLMN including registering on the PLMN.

5.4.3. Provisioning a CSG in the UE's Operator CSG list

The Operator CSG list is read only by the UE and provisioned using OMA DM or OTA procedures. The Operator CSG list is provisioned using the OTA procedures for a UE with a Rel-9 USIM and stored on the USIM as defined in TS 31.102 [9] and using the OMA DM procedures for a pre-Rel-9 USIM as defined in TS 24.285 [11]. Further details of the OMA DM procedures can be found in Section 5.4.2.1.

NOTE: The Operator CSG list is defined using access condition ADM defined in TS 31.102 [9] to ensure that the user or ME are not able to write to the list. ADM is the access condition to an EF file on the UICC which is under the control of the authority which creates this file.

If a message with cause value #25 (see 3GPP TS 24.008 [17] and 3GPP TS 24.301 [16]) is received by the UE then the following applies:

- The NAS shall remove the CSG ID from the Allowed CSG list, if present in the Allowed CSG List; and
- For a CSG ID present in the Operator CSG list, then for an implementation dependent time, until the UE is switched off, the SIM/USIM is removed, or the Operator CSG list is updated:
  - The NAS shall not include this CSG ID and the associated PLMN in the list of Allowed CSG identities and associated PLMN identities provided to the AS;
  - In CSG manual mode selection, the UE shall not indicate that this CSG ID and the associated PLMN is in the Operator CSG List stored in the UE.

One method to implement these procedures is to maintain a list of "forbidden CSG IDs" which is erased when the UE is switched off or when the SIM/USIM is removed, and periodically (with a period in the range 12 to 24 hours). Each CSG entry in the list of "forbidden CSG IDs" shall include a CSG ID and PLMN identity.

In addition, a CSG entry is removed from the list of "forbidden CSG IDs" in the UE if,

a) The UE registers successfully at a CSG cell due to manual CSG selection at a cell corresponding to the CSG entry; or

b) The corresponding CSG entry is removed from the Operator CSG list.

NOTE: There is a requirement in TS 22.220 [8] that the Allowed CSG list and Operator CSG list are maintained independently from each other, i.e., a change in the Operator CSG list shall not trigger the UE to modify the Allowed CSG list to reflect such change automatically. Therefore, when a CSG entry is added or removed from the Operator CSG list, if the same entry occurs in the Allowed CSG list, then the UE keeps the entry in the Allowed CSG list.

5.5. Management of out-of-date CSG information at the UE by the network

5.5.1. General

One issue to consider is how to manage CSG subscription data that is out of synch between the UE and the network. For example, when a CSG subscription has expired for a temporary CSG member or is removed for a permanent CSG member, the entry for this CSG in the Allowed CSG list or Operator 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.

This results in two problems:

1) When paging optimisation is performed, the network may avoid sending paging messages to those CSG cells for which the UE no longer has a CSG subscription. Therefore, the UE may be camped on a CSG cell where it will not be paged.
2) While camped on the cell, the UE gives a false service indication.

In order to solve the first problem, when paging optimisation is supported, the MME/SGSN/MSC/VLR 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 of whether CSG subscription(s) that are stored by MME/SGSN/MSC/VLR are valid or not. Further details can be found in Section 5.5.2.

It is not clear if a solution exists to solve the second problem, but there are two approaches which can be used to minimize the potential false service indication time:

1) An operator with generally good macro coverage does not have to worry about the UE being truly out of coverage since the UE will likely be able to find suitable coverage on another cell when it is rejected at the CSG cell.
2) An operator with poorer coverage will have to update the UE's Allowed CSG list and Operator CSG list more frequently so that the UE does not give a false service indication for very long.

5.5.2. Procedures for managing changes to CSG membership and temporary CSG memberships

When a CSG entry is removed from the CSG subscription data or the CSG membership expires, the following functionality is defined in TS 23.008 [22] to support paging optimization:

- If the CSG entry is removed from the CSG subscription data, then the CSG entry should not be removed at the HSS/HLR before the CSG entry is removed from the UE; rather the CSG expiration date should be modified to an expired date and if applicable the HSS/HLR shall inform the MME/SGSN/MSC/VLR of the expired CSG information.

NOTE: The CSG expiry time set to an expired value will indicate to the MME/SGSN/MSC/VLR that the UE has not updated when the UE was removed from a CSG or the CSG has expired for a temporary membership.

- When the CSG entry is removed from the UE, the HSS/HLR should delete the CSG entry and, if applicable, update the MME/SGSN/MSC/VLR.

NOTE: The removal of the CSG entry from the UE and the HSS/HLR update can be performed independently by different systems. The temporal relationship between the two operations depends on operator policy.

NOTE: If the CSG list server succeeds in removing a CSG from the UE's Allowed CSG list or Operator CSG list via OMA DM or OTA, it informs the HSS via an unspecified interface.

- When the HSS/HLR stores CSG entries with an expired time, these shall also be included in the CSG subscription data sent to the MME/SGSN/MSC/VLR.
- If the MME performs paging optimization and the HeNB is connected directly to the MME, the MME shall page the UE at all CSGs that advertise a TA where the UE may be camped on and which are in the UE's CSG subscription data, including both valid and expired CSG entries.
- If a H(e)NB GW is present, the MME/SGSN/MSC/VLR shall include a list of CSG IDs for paging to support paging optimization. For paging optimization, the CSG IDs of expired CSG subscriptions and valid CSG subscriptions are both included in the list of CSG IDs.
- In addition, if the UE is in connected mode at the CSG cell for which the timer expires or the UE is removed from the CSG, then:
  - The MME/SGSN/MSC/VLR shall send a Context Modification Request or Common ID message to the H(e)NB indicating that the CSG membership of the UE has expired.
  - The H(e)NB receiving this message may initiate a handover to a suitable cell. If the UE is not handed over, the H(e)NB shall release the RRC connection to move the UE to the idle state.

NOTE: If an operator does not deploy OTA/OMA DM, then paging optimization is disabled and the HSS can delete expired CSG IDs directly when they expire, or are removed. It is FFS how to handle cases when the 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).

NOTE: The use of the NAS reject message with cause code #25 (Not authorized for this CSG) sent by the MME/SGSN/MSC to remove a CSG ID from UE's Allowed CSG list will not result in the CSG ID being removed from the CSG subscription data at the HSS.

5.6. CSG Provisioning call flows

5.6.1. Adding or removing a subscriber at a CSG initiated by the CSG manager

An example call flow of adding or removing a subscriber at a CSG initiated by the CSG manager is shown in Figure 5-4.

NOTE: The call flow may apply to a UE in idle or connected mode. In the case of idle mode, it is necessary to page the UE and establish a connection to perform step 8.

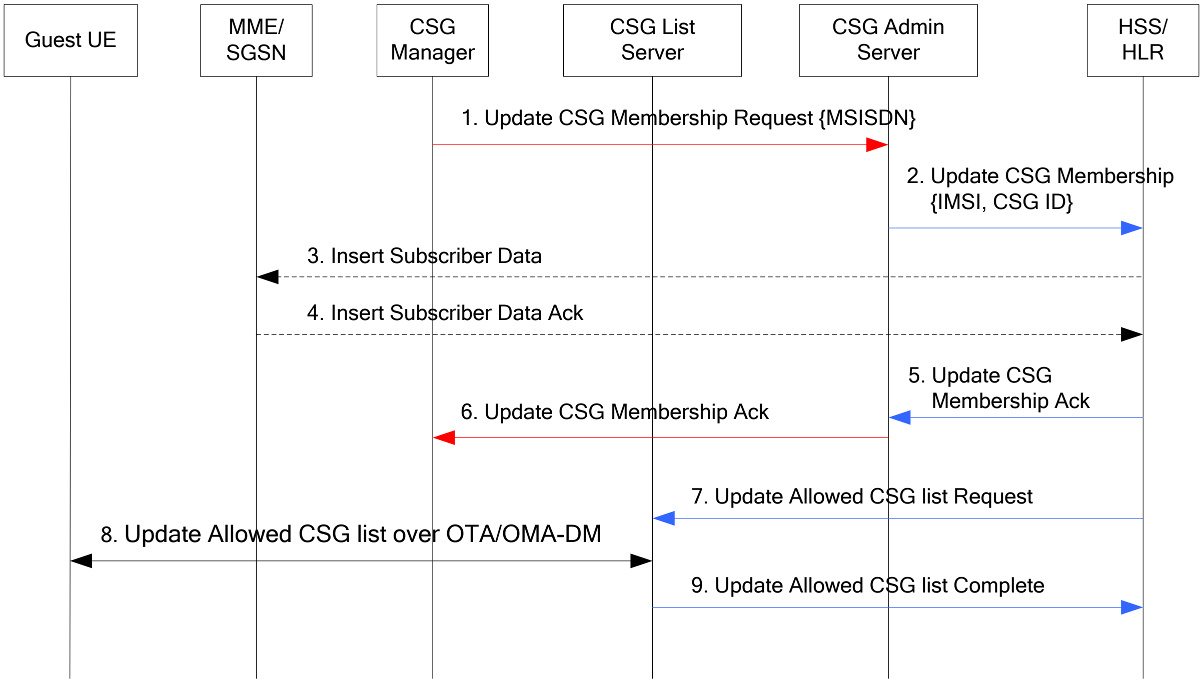
Guest UE
MME/ SGSN
CSG Manager
CSG List Server
CSG Admin Server
HSS/ HLR
1. Update CSG Membership Request {MSISDN}
2. Update CSG Membership {IMSI, CSG ID}
3. Insert Subscriber Data
4. Insert Subscriber Data Ack
5. Update CSG Membership Ack
6. Update CSG Membership Ack
7. Update Allowed CSG list Request
8. Update Allowed CSG list over OTA/OMA-DM
9. Update Allowed CSG list Complete

Figure 5-4: Adding a subscriber at a CSG initiated by the CSG manager

1. The CSG manager sends a request to the CSG Administration Server to add or remove a subscriber to the CSG. For example, the CSG manager logs into a web page with a secure UserID and Password; clicks a Tab on the web page for their CSG; and selects a subscriber to add (including setting an optional time limit for membership) or remove.

2. Adding or removing a subscriber at a CSG is subject to approval by the operator. For example, for adding a user, the CSG Administration Server determines whether to approve the user's subscription to the CSG based on billing models, roaming agreements etc.

   Once approved, the CSG Administration Server communicates with the HSS/HLR to update the subscriber's CSG subscription data stored in the HSS/HLR.

   For adding a UE at a CSG, the UE needs to be provisioned at the CSG Administration Server using a permanent and unique identifier that is preferably easily accessible to the subscriber such as the MSISDN. The MSISDN (or equivalent) is converted to an IMSI for use in the (E)-UTRAN for access control, charging, etc.

   The expiration time may also be set if the CSG manager has set a time limit for membership.

   For removing a UE from a CSG, since the UE has not yet been updated using OMA DM or OTA that the CSG has been removed, the HSS/HLR CSG subscription data for this CSG should be modified to an expired date. Further details can be found in Section 5.5.

NOTE: The CSG Administration Server needs to access the HSS/HLR for the subscriber in order to update the CSG subscription data. In the case of roaming, the CSG Administration Server of the visited network where the CSG is located needs to have access to the HSS/HLR of the subscriber in the home network either directly or indirectly.

3. If the UE is currently attached at an MME/SGSN/MSC/VLR, then the HSS/HLR sends an Insert Subscriber Data (IMSI, Subscription Data) message indicating the change in CSG subscription data.
4. The MME/SGSN/MSC/VLR returns an Insert Subscriber Data Ack message to the HSS/HLR.
5. The HSS/HLR confirms the subscriber has been added or removed to the CSG Administration Server.
6. The CSG Administration Server confirms the subscriber has been added or removed to the CSG manager.
7. The HSS/HLR informs the CSG List Server via an unspecified interface that the UE is added or removed as a member of the CSG in order to trigger the update of the Allowed CSG list or Operator CSG list on the UE.
8. The CSG List Server and UE perform an OMA DM or OTA update of the UE's Allowed CSG list or Operator CSG list.

NOTE: It is left to operator policy whether to add the CSG to the Operator CSG list or the Allowed CSG list. For example, an operator may choose to store operator specific CSG memberships in the Operator CSG list while temporary or user managed CSG subscriptions in the Allowed CSG list. Alternatively, an operator may choose to just use a single list.

9. The CSG List Server notifies the HSS/HLR that the UE's Allowed CSG list or Operator CSG list has been updated successfully via the unspecified interface.

NOTE: In the case that the UE is removed from a CSG, the HSS/HLR should erase the CSG entry from the CSG subscription data and send an Insert Subscriber Data (IMSI, Subscription Data) message to the MME/SGSN/MSC/VLR (not shown) indicating that the CSG has been removed from the UE.

NOTE: In the case of a UE added to a CSG, prior to steps 7-9, the subscriber may perform a manual CSG selection of the CSG cell. Upon selecting the CSG, the UE performs a registration procedure. Further details are not shown for simplicity; see Section 5.4.2.2 for details. If the MME/SGSN/MSC/VLR accepts the UE, the UE will add the corresponding CSG ID to the Allowed CSG list.

If the UE receives an Accept message via a hybrid cell, the UE does not add the corresponding CSG ID to its Allowed CSG List. Adding a CSG ID to the UE's Allowed CSG List for a hybrid cell is performed only by OTA or OMA DM procedures.

NOTE: The update of the Allowed CSG list or Operator CSG list at the UE and the update of the HSS/HLR by the CSG Administration Server can be performed independently by different systems. The temporal relationship between the two operations depends on operator policy.

5.6.2. Adding or removing a subscriber at a CSG initiated by the subscriber

An example call flow of adding or removing a subscriber at a CSG initiated by the subscriber is shown in Figure 5-5.

NOTE: The call flow may apply to a UE in idle or connected mode. In the case of idle mode, it is necessary to page the UE and establish a connection to perform step 8.

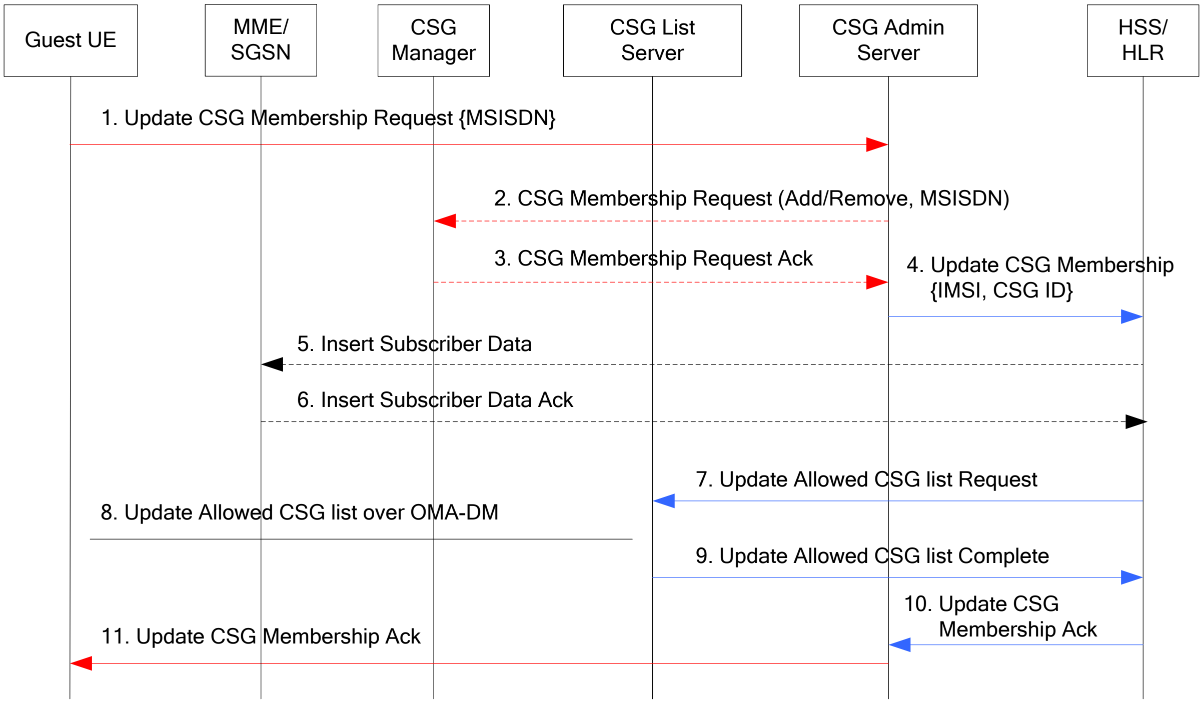
Guest UE
MME/ SGSN
CSG Manager
CSG List Server
CSG Admin Server
HSS/ HLR
1. Update CSG Membership Request {MSISDN}
2. CSG Membership Request (Add/Remove, MSISDN)
3. CSG Membership Request Ack
4. Update CSG Membership {IMSI, CSG ID}
5. Insert Subscriber Data
6. Insert Subscriber Data Ack
7. Update Allowed CSG list Request
8. Update Allowed CSG list over OMA-DM
9. Update Allowed CSG list Complete
10. Update CSG Membership Ack
11. Update CSG Membership Ack

Figure 5-5: Adding a subscriber at a CSG initiated by the subscriber

1. The subscriber sends a request to the CSG Administration Server to add or remove membership in a CSG. For example, the subscriber logs into a web page with a secure UserID and Password; performs a search for CSGs and selects one to request to add or remove CSG membership.
2. Adding or removing a subscriber at a CSG is subject to approval by the operator. For example, for adding a user, the CSG Administration Server determines whether to approve the user's subscription to the CSG based on billing models, roaming agreements etc. If the subscriber meets the operator's approval, the CSG Administration Server forwards the request for membership to the manager of the CSG and waits for a response.

3. The CSG manager accepts the request after some delay.

NOTE: The CSG manager may not be required for explicit approval of CSG membership. For example, the CSG Administration Server may host a web application that requires a subscriber to enter a password, credit card info, etc. to gain automated access. An application like a web browser is ideal in that it provides flexibility to implement many different business models since the web application can request any type of information from the subscriber.

4. Once approved, the CSG Administration Server communicates with the HSS/HLR to update the CSG subscription data stored in the HSS/HLR.

   For adding a UE at a CSG, the UE needs to be provisioned at the CSG Administration Server using a permanent and unique identifier that is preferably easily accessible to the subscriber such as the MSISDN. The MSISDN (or equivalent) is converted at the HSS/HLR to an IMSI for use in the (E)-UTRAN for access control, charging, etc.

   The expiration time may also be set if the CSG manager has set a time limit for membership.

   For removing a UE from a CSG, since the UE has not yet been updated using OMA DM or OTA that the CSG has been removed, the HSS/HLR CSG subscription data for this CSG should be modified to an expired date. Further details can be found in Section 5.5.

NOTE: The CSG Administration Server needs to access the HSS/HLR for the subscriber in order to update the CSG subscription data. In the case of roaming, the CSG Administration Server of the visited network where the CSG is located needs to have access to the HSS/HLR of the subscriber in the home network either directly or indirectly.

5. If the UE is currently attached at an MME/SGSN/MSC/VLR, then the HSS/HLR sends an Insert Subscriber Data (IMSI, Subscription Data) message indicating the change in CSG subscription data.

6. The MME/SGSN/MSC/VLR returns an Insert Subscriber Data Ack message to the HSS/HLR.

7. The HSS/HLR informs the CSG List Server via an unspecified interface that the UE is added or removed as a member of the CSG in order to trigger the update of the Allowed CSG list or Operator CSG list on the UE.

8. The CSG List Server and UE perform an OMA DM or OTA update of the UE’s Allowed CSG list or Operator CSG list.

NOTE: It is left to operator policy whether to add the CSG to the Operator CSG list or the Allowed CSG list. For example, an operator may choose to store operator specific CSG memberships in the Operator CSG list while temporary or user managed CSG subscriptions in the Allowed CSG list. Alternatively, an operator may choose to just use a single list.

9. The CSG List Server notifies the HSS/HLR that the UE’s Allowed CSG list or Operator CSG list has been updated successfully via an unspecified interface.

NOTE: In the case of a UE added to a CSG, prior to steps 7-9, the subscriber may perform a manual CSG selection of the CSG cell to update the Allowed CSG list. Upon selecting the CSG, the UE performs a registration procedure. Further details are not shown for simplicity; see Section 5.4.2.2 for details. If the MME/SGSN/MSC/VLR accepts the UE, the UE will add the corresponding CSG ID to the Allowed CSG list.

> If the UE receives an Accept message via a hybrid cell, the UE does not add the corresponding CSG ID to its Allowed CSG List. Adding a CSG ID to the UE's Allowed CSG List for a hybrid cell is performed only by OTA or OMA DM procedures.

10. The HSS/HLR confirms the subscription has been correctly updated.
11. The CSG Administration Server confirms the subscriber has been added to the CSG.

NOTE: Steps 10 and 11 may be performed any time after step 6 depending on whether the subscriber is to be informed before or after the Allowed CSG list or Operator CSG list on the UE is updated.

NOTE: The update of the Allowed CSG list or Operator CSG list at the UE and the update of the HSS/HLR by the CSG Administration Server can be performed independently by different systems. The temporal relationship between the two operations depends on operator policy.

6. Access control for CSG and hybrid cells

6.1. Access control when establishing a connection at a CSG cell or a hybrid cell

6.1.1. General

For CSG aware UEs (Rel-8 and onwards) the CSG subscription data is permanently stored in the HSS/HLR, and retrieved by the MME, MSC/VLR and SGSN for access control during the attach procedure, service request procedure or tracking/location/routing area updating procedure as part of the UE's subscription profile.

- When a UE accesses a CSG cell, the MME/SGSN/MSC/VLR 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.
- If the CSG ID of the CSG cell is not present in the UE's CSG subscription data or the timer has expired, then the MME/SGSN/MSC/VLR shall send a reject message with the error code #25 (Not authorized for this CSG). The UE shall remove the entry for this CSG from the Allowed CSG list if present.

For non-CSG-aware UEs (UMTS only), the access control list is permanently stored in an OAM function, and pushed to or retrieved by the HNB GW (mandatory) and HNB (optional) for access control. For example, an OAM interface between the CSG Administration Server and the HNB GW and HNB may be used to push or retrieve the access control list.

For CSG cells, the network performs access control based on the CSG ID advertised by the CSG cell and the CSG subscription data of the UE stored in the network. For hybrid cells, the network verifies whether the UE is a CSG member or not.

6.1.2. Access control for CSG-aware UEs at CSG cells and hybrid cells

An example call flow of a registration procedure at a CSG cell or a hybrid cell is shown in Figure 6-1.

NOTE: For simplicity, no details are shown for instance if the S-GW or SGSN/MME changes during the procedure as there is no change to these steps for CSG cells. For further details see the individual Attach, Location Registration (LAU/RAU/TAU), Detach or Service Request procedures in TS 23.060 [1] and TS 23.401 [2].

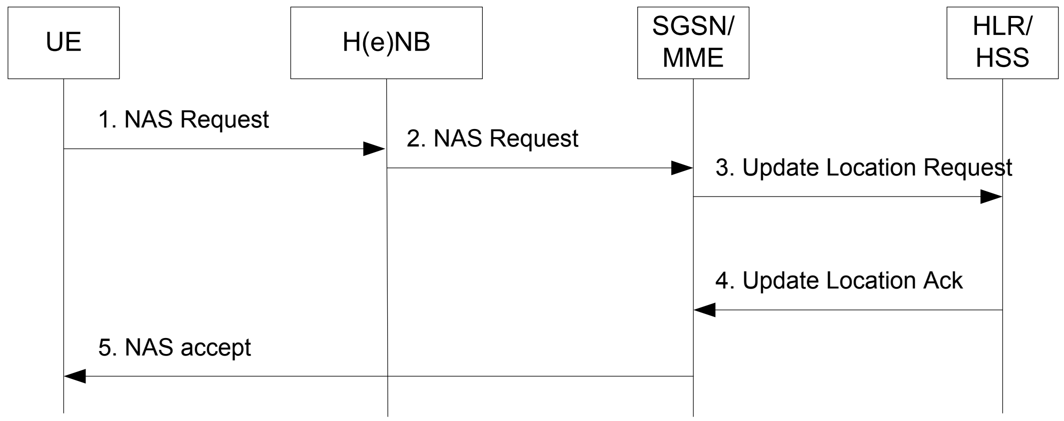

Figure 6-1: Access control at a CSG cell or a hybrid cell

1. The UE initiates the NAS procedure (e.g., Attach, Location Registration (LAU/RAU/TAU), Detach or Service Request) by sending, to the H(e)NB, the appropriate NAS Request.

   For example, the UE initiates the TAU procedure when it detects a change to a new TA that is not in the list of TAIs that the UE registered with the network or the user manually selects the CSG cell that is not in the UE's Allowed CSG list.

2. The H(e)NB forwards the NAS Request message together with the Cell Access Mode, CSG ID, and other information of the cell from where it received the message to the SGSN/MME. The CSG ID is provided by the H(e)NB if the UE sends the NAS Request message via a CSG cell or a hybrid cell. The Cell Access Modes is provided by the H(e)NB if the UE sends the NAS Request message via a hybrid cell.

   For example, the HeNB selects the MME from the GUTI and from the indicated Selected Network and forwards the TAU Request message to the MME along with the CSG ID of the HeNB. In the case where the HeNB is connected to a HeNB GW, the HeNB forwards the TAU Request message to the HeNB GW and the HeNB GW performs the function of selecting the MME from the GUTI and from the indicated Selected Network and forwards the TAU Request message to the MME along with the CSG ID of the HeNB.

NOTE: The HeNB-GW is not shown as it does not play a role in admission control for CSG-aware UEs beyond the network node selection function.

   In addition, when a UE accesses a HNB, the HNB performs the Registration procedure (not shown) to inform the HNB-GW of the specific HNB where the UE is located. The HNB sends the UE Register Request message to the HNB-GW to register the UE at the HNB-GW if the identity of the UE (provided during RRC Connection Establishment) is unknown at the HNB being accessed, i.e. no Context id exists for the UE in the HNB.

3. The SGSN/MME verifies whether it holds subscription data for the UE. If there is no subscription data in the SGSN/MME for this UE then the SGSN/MME sends an Update Location Request message to the HLR/HSS.

4. The HLR/HSS acknowledges the Update Location Request message by sending an Update Location Ack (IMSI, Subscription Data) message to the SGSN/MME. In the case of UMTS, the Subscription Data may be sent before the Update Location Ack using the

Insert Subscriber Data procedures depending on the interface between the SGSN and the HSS/HLR. The Subscription Data may contain the CSG subscription data for the PLMN.

If the UE initiates the NAS procedure at a CSG cell, the SGSN/MME shall check whether the CSG ID is contained in the CSG subscription and is not expired. If the CSG ID is not present or expired, the SGSN/MME shall send the corresponding NAS reject message to the UE with the cause value #25 (Not authorized for this CSG). The UE shall remove the CSG ID from its Allowed CSG list if present. For further details see Sections 5.4.2 and 5.4.3.

For an Emergency Attach the SGSN/MME shall not check for access restrictions, regional restrictions or subscription restrictions (e.g. CSG restrictions). Similarly, if the UE has ongoing emergency bearer services no CSG access control shall be performed.

If all checks are successful then the SGSN/MME constructs a context for the UE.

5. The SGSN/MME sends a NAS Accept message to the UE.

   If the NAS procedure is initiated due to manual CSG selection and occurs via a CSG cell, the UE upon receiving the NAS Accept message shall add the CSG ID to its Allowed CSG list if it is not already present, as described in Section 5.4.2.2.

NOTE: Manual CSG selection is not supported if the UE has emergency bearers established.

If the NAS procedure is performed via a hybrid cell, then the SGSN/MME shall send an indication of whether the UE is a CSG member to the H(e)NB along with the RANAP/S1-MME control message. Based on this information the H(e)NB may perform differentiated treatment for CSG members and non-members.

NOTE: If the UE receives a NAS Accept message via a hybrid cell, the UE does not add the corresponding CSG ID to its Allowed CSG list. Adding a CSG ID to the UE's local Allowed CSG list for a hybrid cell is performed only by OTA or OMA DM procedures.

6.1.3. Access control when the UE or the HNB is not CSG-aware

The UE Registration Function for a HNB provides means for the HNB to convey UE identification data to the HNB-GW in order to perform access control for the non CSG aware UEs in the HNB GW, or for CSG-aware UEs registering through a non-CSG aware HNB. The UE Registration also informs the HNB-GW of the specific HNB where the UE is located.

NOTE: If a deployment is such that a UE can move between the HNBs having the same LAC (for example, in an enterprise deployment), the HNB-GW cannot assume that the UE Registration procedure provides the UE’s location at a specific HNB at any time other than the UE registration time.

NOTE: If the CN is pre-Rel-8, access control could be performed at the HNB-GW.

An example call flow from TS 25.467 [14] of a registration procedure is at a HNB is shown in Figure 6-2.

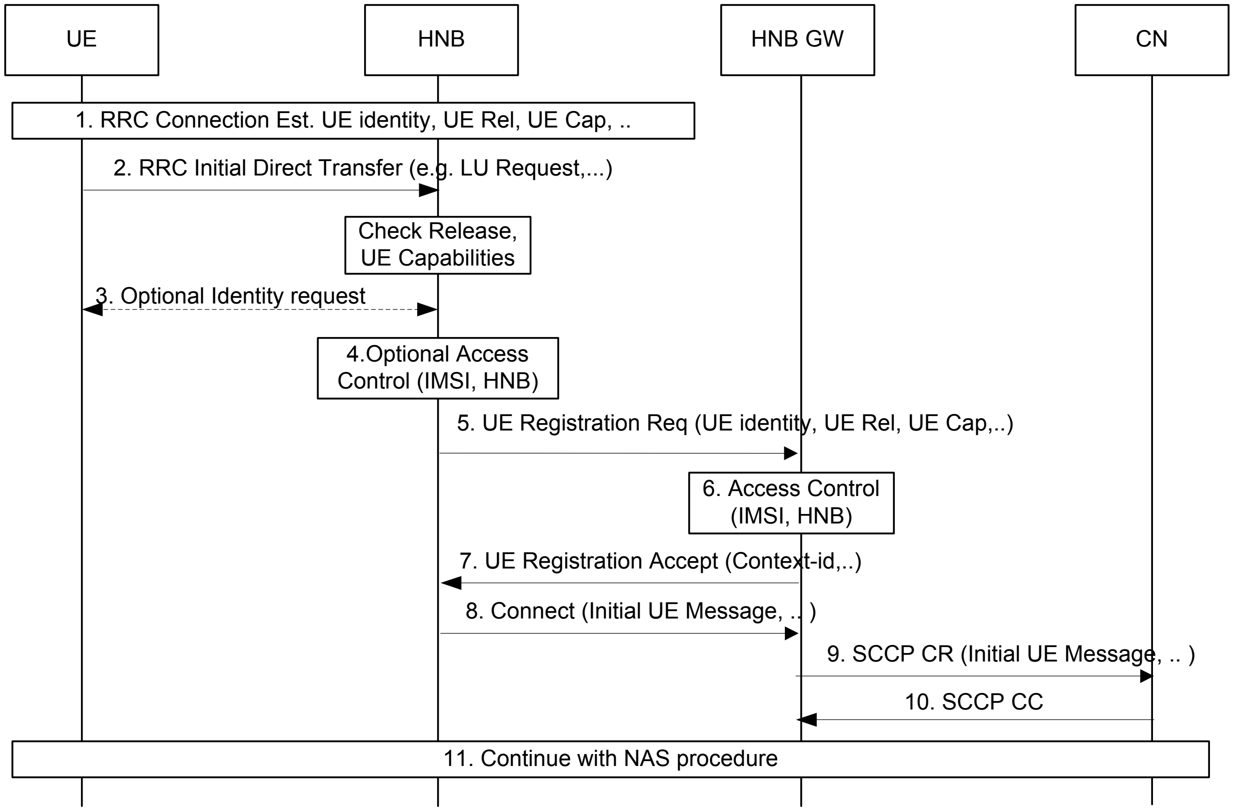
UE
HNB
HNB GW
CN
1. RRC Connection Est. UE identity, UE Rel, UE Cap, ..
2. RRC Initial Direct Transfer (e.g. LU Request,...)
Check Release, UE Capabilities
3. Optional Identity request
4.Optional Access Control (IMSI, HNB)
5. UE Registration Req (UE identity, UE Rel, UE Cap,..)
6. Access Control (IMSI, HNB)
7. UE Registration Accept (Context-id,..)
8. Connect (Initial UE Message, ..)
9. SCCP CR (Initial UE Message, ..)
10. SCCP CC
11. Continue with NAS procedure

Figure 6-2: Access control for non-CSG-aware UEs at CSG cells or non-CSG HNBs

1. Upon camping on the HNB, the UE initiates an initial NAS procedure (e.g. LU Procedure) by establishing an RRC connection with the HNB. UE identity, UE capabilities, e.g. "Access stratum release indicator" or “Support of CSG” and Establishment Cause, are reported to the HNB as part of the RRC Connection establishment procedure.

2. The UE then transmits a RRC Initial Direct Transfer message carrying the initial NAS message (e.g. Location Updating Request message) with some form of UE identity.

3. The HNB checks the UE capabilities provided in step 1, and if these indicate that CSG is not supported, or the HNB itself does not support CSG, and if the identity of the UE (provided during RRC Connection Establishment) is unknown at the HNB being accessed, i.e. no Context id exists for the UE, the HNB initiates UE registration towards the HNB-GW (step 5-7).

   Before starting the UE Registration procedure, the HNB triggers the Identification procedure (step 3) asking the UE for its IMSI, unless that identity has already been provided during the RRC Connection Establishment. The Identification procedure may also be skipped for an emergency call.

   If the HNB has a context id for the UE, the UE registration procedure is not performed nor is the Identification procedure.

4. The HNB may optionally perform access control based on the provided IMSI and the provided access control list

5. The HNB attempts to register the UE on the HNB-GW by transmitting the UE REGISTER REQUEST. The message contains at a minimum:

   - **UE Identity**: a unique identity for the UE provided in step 1 or 3.

   - **UE Capabilities**: derived from that provided in step 1.

   —**Registration Cause:** indicates whether a UE registration is for an emergency call.

NOTE: The UE Identity provided in the HNBAP UE REGISTER REQUEST message is unauthenticated.

6. The HNB-GW checks the UE capabilities and the Registration Cause and performs access control for the following cases for the particular UE attempting to utilize the specific HNB:

   - If the UE is not CSG-ware.

   - If the HNB operates in closed access mode and does not support the CSG concept.

   Access control is skipped if the Registration Cause indicates an emergency call.

7. If the HNB-GW accepts the UE registration attempt it shall allocate a context-id for the UE and respond with a HNBAP UE REGISTER ACCEPT message, including the context-id, to the HNB.

   If the HNB is a hybrid cell, then the HNB-GW also includes the CSG Membership Status in the HNBAP UE REGISTER ACCEPT message.

   If the HNB-GW chooses not to accept the incoming UE registration request then the HNB-GW shall respond with a HNBAP UE REGISTER REJECT message. The HNB behaviour for reject handling shall further be determined by the cause specified in the HNBAP UE REGISTER REJECT message.

8. The HNB then sends an RUA CONNECT message containing the RANAP Initial UE message.

9. The reception of the RUA CONNECT message at the HNB-GW triggers the setup of an SCCP connection by the HNB-GW towards the CN. The HNB-GW then forwards the RANAP Initial UE Message to the CN.

10. The CN responds with an SCCP Connection Confirm message.

10a. The HNB-GW shall additionally utilize a CN assisted method if available (e.g. using IMSI provided in the COMMON ID message), to alleviate the security risks associated with spoofing of IMSI and can subsequently trigger a UE deregistration upon detection of such an event.

11. The UE continues with the NAS procedure (e.g. Location Updating procedure) towards the CN, via the HNB and the HNB-GW.

6.2. Access control for in-bound handover to a CSG cell or hybrid cell

6.2.1. Access control for in-bound handover for CSG aware UEs

In-bound handover is defined as a common solution in the following handover scenarios:

- Intra-RAT inbound mobility to a H(e)NB (CSG cell or hybrid cell).
- Inter-RAT inbound mobility to a H(e)NB (CSG cell or hybrid cell).

Figure 6.2-1 shows the call flow for inbound handover using the messages currently defined in RANAP/S1-AP.

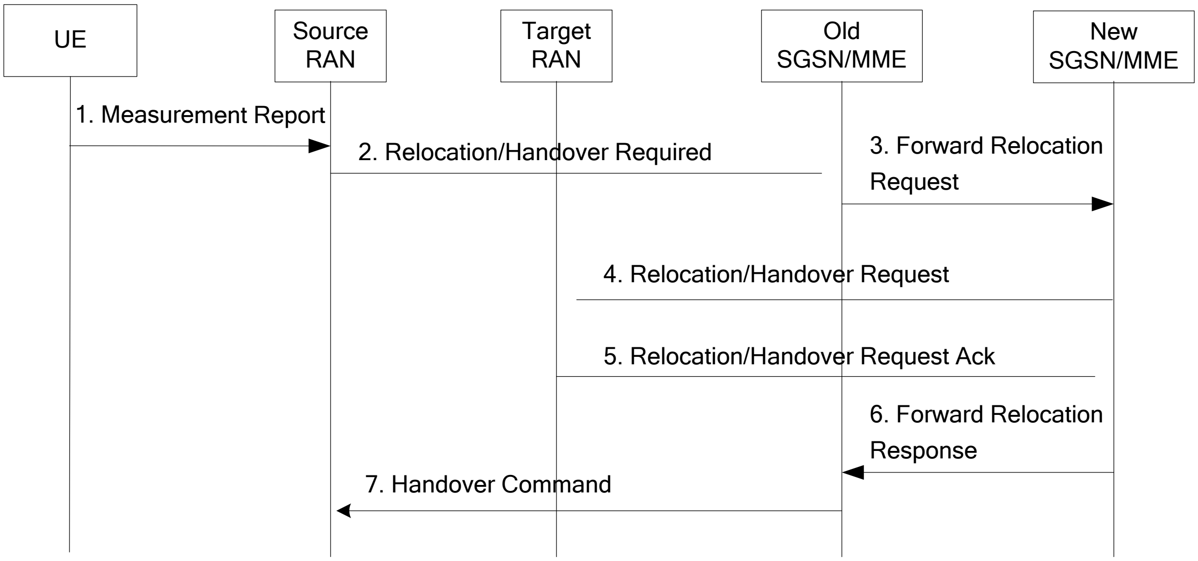
UE
Source RAN
Target RAN
Old SGSN/MME
New SGSN/MME
1. Measurement Report
2. Relocation/Handover Required
3. Forward Relocation Request
4. Relocation/Handover Request
5. Relocation/Handover Request Ack
6. Forward Relocation Response
7. Handover Command

Figure 6-3: Access control options in the Core Network for in-bound mobility

1. The UE reads the CSG ID, access mode and Cell Global ID (CGI)/Cell Identity of the target cell and compares the CSG ID of the target cell to the CSG Whitelist to determine if the UE is a member of the CSG advertised by the target cell as defined in Section 7.4.1. The UE reports the CGI/Cell Identity and the CSG Membership status associated with the target cell, in the measurement report.

2. For a target cell that is a CSG cell, if the UE indicates it is member of the CSG, then the source RAN initiates the handover and sends a Relocation/Handover Required message to the old SGSN/MME.

For a target cell that is a hybrid cell, the source RAN initiates the handover and sends a Relocation/Handover Required message to the old SGSN/MME.

The source RAN includes the CSG ID when the target cell is a CSG cell or a hybrid cell. The source RAN indicates the Cell Access Mode when the target cell is a hybrid cell.

3. The old SGSN/MME determines from the Target ID if the relocation is an intra-SGSN/MME relocation or an inter-SGSN/MME relocation. In case of inter-SGSN/MME relocation/handover the old SGSN/MME initiates the relocation resource allocation procedure by sending a Forward Relocation Request message to the new SGSN/MME.

If the CSG ID is provided by the source RAN, the old SGSN/MME shall check whether the CSG ID is contained in the CSG subscription and is not expired. If the CSG ID is not present or is expired and the target cell is a CSG cell, the old SGSN/MME shall reject the handover with an appropriate cause.

If the target cell is a CSG or hybrid cell, the old SGSN/MME includes the CSG ID in the Forward Relocation Request message. If the target cell is a hybrid cell, the old SGSN/MME includes the CSG Membership Status indicating whether the UE is a CSG member in the Forward Relocation Request message.

4. The new SGSN/MME sends a Relocation/Handover Request message to the target RAN via the H(e)NB GW if present. The new SGSN/MME shall include the CSG ID and CSG Membership Status when provided by the old SGSN/MME in the Forward Relocation Request message.

5. The target RAN confirms the CSG ID and access mode and sends the Relocation/Handover Request Acknowledge message to the new SGSN/MME via the H(e)NB GW if present.

   The target RAN shall verify the CSG ID provided by the source RAN. If the target cell is a CSG cell and the CSG ID provided by the source RAN does not match the CSG ID of the target cell, the target cell shall reject the handover with an appropriate cause.

   If the target cell is a hybrid cell and the CSG ID provided by the source RAN does not match the CSG ID of the target cell, the target cell accepts the handover and the H(e)NB may provide the QoS to the UE as for a non member. In addition the H(e)NB and shall include the actual CSG ID broadcast by the target cell Relocation/Handover Request Acknowledge message.

   If the target cell is a hybrid cell and differentiated treatment of CSG and non-CSG members is performed, then the CSG membership status is used to differentiate CSG and non-CSG members.

6. If the SGSN/MME has been relocated, the new SGSN/MME sends a Forward Relocation Response message to the old SGSN/MME.

7. The old SGSN/MME sends a Handover Command message to the source RAN.

6.2.2. Access control for in-bound handover for non-CSG aware UEs

TS 25.467 [14] defines in-bound handover for non-CSG UEs in the following scenario:

- The UE is non-CSG capable and not able to read SIBs for CSG inbound mobility purposes.
- The HNB-GW is able to perform CSG membership verification for the UE.
- The HNB-GW is able to route the incoming relocation to the appropriate target HNB.

In this scenario the source RAN uses the relocation procedures as defined in TS 23.060 [1] and TS 25.413 [32] except the source RAN shall not include the CSG ID and the Cell Access Mode of the target cell in the Relocation Required message. As a result, the SGSN does not perform any access control for the UE and instead it is performed by the HNB-GW when it receives a Relocation Request message that does not include the target CSG ID and the CSG Membership Status. In addition the HNB GW initiates the HNB-GW Triggered UE Registration with the HNB. If the target HNB is a hybrid cell, the HNB GW uses CSG membership status to differentiate between members and non- members of the cell. For further details see TS 25.467 [14].

6.3. Differentiating between a CSG member and a non-CSG member at a hybrid cell

TS 22.220 [8] defines the following requirements related to QoS support for hybrid cells:

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

Based on this requirement, the following principles apply to serving non CSG members and CSG members at a hybrid cell:

- When the UE connects or performs a handover to a hybrid cell, the MME/SGSN informs the serving H(e)NB whether the UE is a member or not of the CSG associated with this hybrid cell;
- Based on CSG membership, the offered QoS for UEs served by this hybrid cell may be modified as follows:
  - The hybrid cell may distinguish between a CSG member and non-member when determining whether to handover a UE, which GBR bearers to admit and which GBR bearers to deactivate;
  - The hybrid cell may distinguish between a CSG member and non-member for handover and packet scheduling on Uu interface (including reduced QoS) of non-GBR bearers.

The CN indicates whether the UE is a member of the CSG as defined in TS 25.413 [32] and TS 36.413 [15] for the following cases:

- The SGSN/MME includes the *CSG Membership Status* IE when the UE establishes a connection at the hybrid cell using the Common ID message (Iu) or the Initial Context Setup Request message (S1);
- The SGSN/MME includes the *CSG Membership Status* IE when the UE performs a Handover to a hybrid cell using the Relocation Required message (Iu) and the Handover Request message (S1); and
- The SGSN/MME may include the *CSG Membership Status* IE when the UE's CSG membership status changes while the UE is connected at the hybrid cell using the Common ID message (Iu) or the UE Context Modification Request (S1).

7. Mobility management for CSG and hybrid cells

7.1. General

The following mobility aspects need to be considered for CSG and hybrid cells:

1. CSG related broadcast parameters
    - CSG related identification parameters
    - CSG related search parameters
2. Idle Mode Cell selection in the presence of CSG and hybrid cells
3. Idle Mode Cell reselection in the presence of CSG and hybrid cells
    - Measurement of CSG and hybrid cells
    - Ranking and reselection for a CSG or hybrid cell
4. Connected Mode Handover to/from/between a CSG or hybrid cell

NOTE: In addition to normal cell selection rules, UEs may perform manual CSG selection as described in Section 5.4.2.2.

7.2. CSG related broadcast parameters

The CSG related parameters broadcast by a H(e)NB can be divided into two categories:

- **CSG related identification parameters**: To support the UE in identification of CSG or hybrid cells.
- **CSG related search parameters**: To support the efficient search of CSG cells.

7.2.1. CSG related identification parameters

In order to support the identification of CSG and hybrid cells, the following CSG related identification parameters are defined in TS 25.331 [33] and TS 36.331 [34]:

- **CSG Indicator:** Indicates that the UE is allowed to access the cell only if the CSG Identity broadcast by the cell is present in the Allowed CSG list or the Operator CSG list stored in the UE. (Note that the union of these two lists is called the “CSG Whitelist” in the access stratum).

  - In UMTS, the CSG Indicator is broadcast by CSG cells only. If the CSG Indicator is absent, the UE considers the cell to be an open or a hybrid cell depending on whether the cell also broadcasts a CSG ID.
  - In LTE, the CSG Indicator is broadcast by all cells. If this indicator is set to TRUE, the UE considers the cell to be a CSG cell. If this indicator is set to FALSE, the UE considers the cell to be an open cell or a hybrid cell depending on whether the cell also broadcasts a CSG ID.

- **CSG Identity (CSG ID):** Identity of the Closed Subscriber Group within the primary PLMN the cell belongs to. The IE is present in CSG and hybrid cells, otherwise the IE is absent and the cell is an open cell. All the CSG or hybrid cells serving the same CSG share the same CSG ID unique within the PLMN.
  - The same CSG ID may identify CSG cells for both UMTS and LTE within a PLMN, i.e., an operator shall not reuse the same CSG ID between UMTS and LTE for different CSGs within a PLMN.
- **HNB Name:** A text based name for the H(e)NB sent only by CSG and hybrid cells. The UE may display the HNB Name, if present, when camping on the cell where it is broadcast. The HNB Name is also used for manual CSG selection.
  - According to TS 22.220 [8], the HNB Name is configurable by the operator or the H(e)NB Hosting Party at the discretion of the operator.

NOTE: There is no requirement that the HNB Name be unique to the CSG, so a user may become confused if there are 2 CSG cells nearby that have different CSG IDs but advertise the same HNB Name. Therefore, it is recommended that an operator manages the configuration of the HNB Name to be unique to the CSG, i.e. the same HNB Name is not reused across CSGs.

> An operator may allow different CSG cells within a CSG to advertise different HNB Names, for example “Enterprise A Meeting Room 1” and “Enterprise A Meeting Room 2”

NOTE: Only CSG and hybrid cells broadcast a CSG ID or HNB Name.

NOTE: In addition to the HNB Name there is also a CSG Type configured by the operator which is stored in the UE in the Allowed CSG list or the Operator CSG list and which is not broadcast by a cell. The CSG Type allows, for example, information on the applied billing regime to be given to the user.

> When present, the CSG Type is displayed when the UE is camped on a CSG or hybrid cell corresponding to that CSG entry. The CSG Type is stored in the USIM or in the ME depending on whether the UE is configured using OTA or OMA DM procedures as described in Sections 5.4.2 and 5.4.3. When the CSG Type is present in the USIM, the CSG Type stored in the ME is ignored. Similarly, if the CSG Type is present in the Operator CSG list, a CSG Type present in the Allowed CSG list is ignored.
>
> The CSG Type is text and/or graphical format (OTA only). When the CSG Type has a text component, the CSG Type text length does not exceed 12 characters in any language.

7.2.2. CSG related search parameters

In order to support the search of CSG cells, the following CSG related search parameters are defined in TS 25.331 [33] and TS 36.331 [34]:

- **CSG PSC/PCI split information:** The set of primary scrambling codes (UMTS) or physical cell identifiers (LTE) reserved for identifying CSG cells on a frequency. The CSG PSC/PCI split information is only valid on the carrier on which it was received in that PLMN. The information may only be assumed valid for 24 hours.
- **Dedicated CSG frequency list (UMTS only):** Specifies the frequencies dedicated for UMTS CSG cells only.

There are 2 possible choices for broadcasting the CSG PSC/PCI split information to the UE:

1. CSG PSC/PCI split information is broadcast at CSG and non-CSG cells
2. CSG PSC/PCI split information is broadcast only at CSG cells.

For optimal performance both CSG and non CSG cells should broadcast the CSG PSC/PCI split information. However, if no changes to the macro network are desired, then broadcasting the information only at CSG cells may require a UE to store the information read at a CSG cell. If the UE does not have any stored information on CSG PSC/PCI split information, then the UE behaviour as to how to identify the presence of CSG cells in its vicinity is based on UE implementation. The UE can use the CSG PSC/PCI split information for search or avoidance of CSG cells.

7.2.3. Summary of CSG related broadcast parameters

CSG Information IE	Broadcast in	Sent by
CSG Indicator	MIB (UMTS) SIB1 (LTE)	CSG cells only (UMTS) CSG cells {TRUE}, open and hybrid cells {FALSE} (LTE)
CSG Identity	SIB 3 (UMTS) SIB1 (LTE)	CSG and hybrid cells only (UMTS and LTE)
HNB Name	SIB 20 (UMTS) SIB9 (LTE)	CSG and hybrid cells only (UMTS and LTE)
CSG PSC/PCI Split Information	SIB 3 or SIB 11bis (UMTS) SIB4 (LTE)	Optional for non-CSG cells and mandatory for CSG cells (UMTS and LTE)
Dedicated CSG frequency list	SIB 11 bis (UMTS only)	Optional for non-CSG cells and CSG cells (UMTS)

7.3. Idle mode procedures for a CSG or a hybrid cell

7.3.1. Cell selection in the presence of CSG and hybrid cells

The normal cell selection rules, i.e. initial cell selection, stored information cell selection and cell selection after leaving connected mode defined in TS 25.304 [4] and TS 36.304 [3] apply in the presence of CSG and hybrid cells.

The NAS may control the cell selection by providing a CSG Whitelist which is the combined Allowed CSG list and Operator CSG list to the AS for the UE to determine whether a CSG cell is suitable for cell selection.

- A CSG cell is not suitable if the CSG ID is not in the CSG Whitelist
- There is no change to suitability definition for a hybrid cell

Stored information cell selection may make use of CSG stored information such as the CSG PSC/PCI split information, if available in the UE.

7.3.2. Cell reselection in the presence of CSG and hybrid cells

For cell reselection a UE sees three different types of cells:

- **Member cell:** A CSG cell or a hybrid cell which advertises a CSG ID that is present in the UE's CSG Whitelist.
- **Normal cell:** A cell which does not advertise a CSG ID or a hybrid cell which advertises a CSG ID that is present in the UE's CSG Whitelist.
- **Non-allowed CSG Cell:** A CSG cell which advertises a CSG ID that is not present in the UE's CSG Whitelist. A non-allowed CSG cell is considered to be not suitable by the UE.

Cell reselection in the presence of CSG and hybrid cells defines an autonomous search function which is intended to find member cells when normal measurement rules are unable to find the member cell. For example, normal measurement rules will not find the member cell when the serving cell is above $S_{intersearch}$.

The autonomous search function is not specified and left to UE implementation. For example, it may rely on geographic triggers (e.g. cell ID of the camped macro cell), periodic searches or some combination of triggers in order to find the Member cell. The autonomous search for Member cells may also include Member cells of other RATs

A UE with an empty CSG Whitelist shall disable the autonomous search function.

7.3.2.1. Measurement rules for CSG and hybrid cells

In addition to the measurement rules specified in TS 25.304 [4] and TS 36.304 [3] for triggering intra-frequency and inter-frequency measurements to a Normal Cell, the UE uses the following measurement rules for triggering intra-frequency and inter-frequency measurements to a Member Cell:

- A UE may ignore or not perform measurements of CSG cells identified by the PSC/PCI split information if no Member Cells are expected to be found in the neighbourhood. For example, if the CSG Whitelist is empty or no Member cells are expected to be found in the neighbourhood.
- A UE camped on a Normal Cell is expected to use the autonomous search function to detect the presence of previously visited suitable intra/inter-frequency Member Cells, even when the measurement rules do not require the UE to perform measurements
- A UE camped on a Member Cell shall use normal measurement rules for intra-frequency CSG or hybrid cells
- A UE camped on a Member Cell may use the autonomous search function for inter-frequency Member Cells

With regard to the interaction with the Frequency/RAT absolute priority feature defined in TS 25.304 [4] and TS 36.304 [3], the UE shall apply an implicit priority to Member cells. In particular:

- For a UE camped on a Normal Cell, inter-frequency or inter RAT Member Cells shall be regarded as if they were on a higher absolute priority frequency layer than the serving one.
- For a UE camped on a Member Cell, inter-frequency or inter RAT Normal Cells shall be considered to have a lower priority than the current frequency layer.

7.3.2.2. Ranking and reselection of CSG and hybrid cells

For intra-frequency cell ranking and reselection, a UE shall use the ranking rules specified in TS 25.304 [4] and TS 36.304 [3] with the following exceptions:

- The UE may ignore any cell belonging to the PCI range allocated to CSG cells. For example, if the CSG Whitelist is empty or none of the CSG cells in the CSG Whitelist are expected to be found in the neighbourhood, as indicated by the autonomous search function.
- If the highest ranked cell is a non-allowed CSG cell, the UE shall not consider this cell as candidate for cell reselection but shall continue to consider other cells on the same frequency for cell reselection
- If the highest ranked cell is a Member cell, the UE shall reselect to that cell.
- If a Member cell is found to be not highest ranked, no action is taken.

For inter-frequency cell ranking and reselection, the UE shall apply an implicit highest priority to ranking of CSG cells where:

- A UE camped on a Normal Cell: If the UE finds a Member cell on any frequency, and the Member cell is the highest ranked on its frequency, the UE shall reselect to the Member cell irrespective of the configured frequency priorities.
- A UE camped on a Member Cell shall consider the frequency of the current cell to be the highest priority frequency as long as the UE remains camped on the Member Cell.
  - Due to this implicit highest priority, as long as the camped Member cell stays strong, the UE need not measure any other frequencies.
  - If the UE detects another Member Cell on a non-serving frequency, the UE may reselect to the detected Member Cell (in an implementation dependent manner) if it is the highest ranked cell on its frequency

LTE has also defined new RSRQ handling procedures to help deal with the case of a UE moving close to a non-allowed CSG cell. In such a case, the macro signal may experience high interference from the non-allowed CSG cell, leading to degraded service. This problem is addressed by adding RSRQ to the cell suitability and search criteria. Given that the RSRQ metric (dB) captures the interference aspect better than the RSRP metric (dBm); the macro cell will no longer be suitable in the presence of a non-allowed CSG interferer. This will force the UE to select other frequencies or RATs, and recover from the degraded service scenario. The associated RSRQ thresholds are network controlled through system information.

NOTE: The above problem is specific to LTE, as UMTS had already defined the equivalent RSRQ criterion.

7.4. Connected mode procedures for a CSG or a hybrid cell

7.4.1. Handover to a CSG or a hybrid cell

While the UE is in connected state, the UE performs normal measurement and mobility procedures based on configuration provided by the network as defined in TS 25.331 [34] and TS 36.300 [7].

In addition, in order to support handover from a source RAN node to a target H(e)NB follows the normal HO procedures with the following exceptions:

1. **PSC/PCI Confusion:** Due to the typical cell size of H(e)NBs being much smaller than macro cells, there can be multiple H(e)NBs within the coverage of the source RAN node that have the same PSC/PCI. This leads to a condition referred to as PSC/PCI confusion, wherein the source RAN node is unable to uniquely determine the target cell for handover from measurement reports received from the UE. PSC/PCI confusion is solved by the UE

reporting the global identity of the target cell. Upon receiving a command from the network, the UE reads the system information of the target cell and reports it back to the network. In order to read the information, the UE creates autonomous gaps temporarily aborting communication with the serving cell.

2. **Proximity Estimation**: In order to report the global identity of the target cell, the UE needs to first read the SI of the target cell. To do this the UE detects using the autonomous search function if it is likely to be in the coverage of a CSG or hybrid cell whose CSG ID is in the UE's CSG Whitelist. Depending on UE capabilities, the UE may then provide the source cell with an indication of proximity to trigger handover preparation if needed. Based on this proximity indication, the source cell may configure the UE to perform the measurement and the reporting necessary for HO.

NOTE: The network configures the UE to enable or disable the sending of proximity indication for a certain RAT.

NOTE: The UE is not expected to provide a proximity indication for a cell whose CSG ID is not in the UE's CSG Whitelist or for a cell that the UE has not visited previously. The configuration of measurements to provide mobility in such cases is up to network implementation.

NOTE: For intra-frequency handovers, UMTS UEs can detect the presence of HNBs, resolve PSC Confusion and assist access control (see below) without the assistance of Proximity Estimation.

3. **Access Control:** The membership status of the UE in the CSG of the target H(e)NB is important for HO. For the case when the target cell is a CSG cell, HO should be performed only if the UE is a member. For the case when the target cell is a hybrid cell, the prioritization of allocated resources may be performed based on the UE's membership status. Access control is done by a two step process, where first the UE reports the membership status based on the observed CSG ID and CSG Whitelist, and then the network verifies the reported status. The network access control is described in Section 6.2.1.

   - The UE reports the following information for the target cell:
     - For target cell in EUTRAN: Cell Global ID, TAC, CSG ID, and CSG Member Status
     - For target cell in UTRAN: Cell Identity, CSG Member Status and CSG ID (if requested by the network). In case of (H)eNB to HNB handovers, the Cell's PLMN, LAC, RAC can be acquired via ANR.
   - If the target cell is a CSG cell, HO should be initiated only if the CSG Member status reported by the UE is positive.

7.5. Registration and paging for CSG cells

7.5.1.Registration for CSG cells

NOTE: Registration procedures for hybrid cells are the same as for normal cells.

There are two modes of CSG selection that impact NAS registration procedures as defined in TS 23.122 [5] :

- **Automatic mode:** This mode utilizes the Allowed CSG list and Operator CSG list, i.e. the CSG Whitelist. The UE camps on a CSG cell only if it is a CSG cell with a CSG identity that is in the Allowed CSG list or Operator CSG list.
    - The idle mode procedures of NAS are not impacted by this mode and normal location/routing area updates (UMTS) and tracking area updates (LTE) continue to apply
        - For UMTS, a CSG aware UE considers itself registered to the location/routing area where the UE last registered and does not need to trigger a location/routing area update other than the periodic location/routing area update as long as it stays in a cell that belongs to the same location/routing area.
        - For LTE, a CSG aware UE considers itself registered to a list of tracking areas stored in its TAI list and does not need to trigger a tracking area update other than the periodic tracking area update as long as it stays in a cell that has one of the tracking areas in the TAI list.
    - A CSG aware UE shall treat all CSG cells where corresponding CSG is not in the Allowed CSG list or Operator CSG list of the UE as though they are NOT a suitable cell.
    - The UE prioritizes camping on Member cells through implicit frequency priority and the autonomous search function, as described in Section 7.3.
- **Manual mode:** In this mode, the UE indicates to the user the list of available CSGs and the associated PLMNs across supported RATs and frequencies. The list of CSGs presented to the user is not restricted by the Allowed CSG list or Operator CSG list stored in the UE. After the user makes a selection, the UE camps on a cell with the selected CSG identity and shall perform an Attach or Location Registration procedure (LAU/RAU/TAU) if the CSG ID of the manually selected CSG cell is not in the Allowed CSG list of the UE. Further details can be found in Section 5.4.2.2.

NOTE: The UE needs to perform a NAS registration procedure when manually selecting a CSG cell not in the Allowed CSG list or Operator CSG list even if the location/routing/tracking area does not require the UE to register. This is because the NAS registration procedure will confirm whether the UE is actually allowed access to the CSG cell, i.e., whether the CSG is in the UE's CSG subscription data on the network and either the Allowed CSG list or Operator CSG list on the UE is out of sync. Otherwise if a UE camps at a CSG cell where it is not allowed and does not perform the NAS registration procedures, then the UE will not be reachable for paging if it is not a member of the CSG.

NOTE: The UE does not need to perform a registration when manually selecting a hybrid cell if the location/routing/tracking area does not require the UE to register.

7.5.2. Paging for CSG cells

NOTE: Paging procedures for hybrid cells are the same as for normal cells.

For non-CSG cells, including hybrid cells, the MME/SGSN/MSC/VLR pages the UE in all cells that the UE is registered to.

For CSG cells, there may be many CSG cells which the UE is not allowed to camp on, but that advertise a location/routing/tracking area for which the UE is registered. It is preferable to optimize the paging by not paging the UE on such cells. This function is called Paging Optimization.

When the HeNB GW is not present, if the MME is configured to support paging optimisation, then the MME should avoid sending Paging messages to CSG cells for which the UE does not have a CSG subscription.

Otherwise, the paging at CSG cells is managed by the H(e)NB-GW and is left to implementation. If the MME/SGSN/MSC/VLR and H(e)NB GW are configured to support paging optimisation, the list of CSG IDs for paging is included in the Paging message sent to the H(e)NB GW. The H(e)NB GW may avoid sending Paging messages to CSG cells for which the UE does not have a CSG subscription, i.e., for CSG cells not included in the list of CSG IDs received.

For paging optimisation, the CSG IDs of expired CSG subscriptions and valid CSG subscriptions are both included in the list.

NOTE: An expired CSG subscription indicates that the UE is not allowed service in the CSG. However, since the removal of the CSG from the UE is pending, it is possible the UE will camp on that CSG and therefore the UE is still paged for the CSG. For further details see Section 5.5.

7.5.3. Configuring TAI/LAI/RAIs for cells under a H(e)NB GW

For UMTS, a LAI/RAI advertised by a NodeB identifies the set of SGSNs that may serve a UE at that NodeB. Any NodeB advertising the same LAI/RAI identifies the same set of SGSNs. This restriction limits how LAI/RAIs may be assigned to HNBs and how they can be reused when non CSG aware UEs are present.

- For example, a non CSG aware UE that registers at a first CSG where it is not a member, may be rejected with a #12 (Location Area not allowed) or # 15 (No Suitable Cells In Location Area) cause code. If the UE is a member of a second CSG with a CSG cell advertising the same LAI/RAI as the first CSG cell, then the UE will avoid camping on a CSG cell in the second CSG until the LAI/RAI is removed from list of forbidden location areas. Therefore, in a network that supports non CSG aware UEs, it is recommended to not reuse Location or Routing Areas as far as possible, and to not use the same Location or Routing Areas for HNBs as for NodeBs.

In LTE, there are no restrictions on the assignment of TAIs for CSG cells with respect to other CSG cells or non-CSG cells with the following exception:

- If a HeNB GW is deployed, the TAI identifies the HeNB GW that serves the HeNB under the MME for routing a Handover Request message for S1 HO; unlike the case of an eNB which is identified by the eNB ID. Therefore different HeNB-GWs need to use different TAIs in order to route the handover messages to the correct HeNB GW.

8. IMS Emergency Session Support at CSG or hybrid cells

8.1. Introduction

There are two aspects of IMS Emergency Session support that need to be considered for CSG or hybrid cells namely:

- IMS Emergency Session Support at a CSG or hybrid cell, i.e., emergency session support related to a UE accessing a CSG or hybrid cell for an emergency service.
- IMS Emergency Session Support at a H(e)NB, i.e., emergency session support related to the fact that a H(e)NB is consumer deployed device and the various issues required to determine location information based on local regulations.

NOTE: The location related and other non CSG issues related to IMS Emergency Session Support at H(e)NBs are undefined as of the completion of Rel-9.

TS 23.060 [1] and TS 23.401 [2] include IMS Emergency Session Support for normal attached UEs and, depending on local regulation, for UEs that are in the limited service state. To acquire emergency services the following procedures apply to the UE:

- A UE camped normally on a cell initiates the normal initial attach procedure if not already attached. An attached UE will initiate the UE Requested PDN Connectivity procedure to receive emergency bearer services.
- A UE in limited service state initiates the Attach procedure indicating that the attach is being performed to receive emergency services.

NOTE: If the network supports emergency services for a UE in limited service, then the network will provide emergency bearer services to the UE independently of whether the UE can be authenticated, has roaming or mobility restrictions or a valid subscription depending on local regulation. Depending on local regulation and an operator's policy, the MME may allow or reject the emergency attach request.

8.2. IMS Emergency Session Support at a CSG or hybrid cell

There are two cases to consider for emergency services support for a UE at a CSG and a hybrid cell namely:

- A UE camped on an allowed CSG cell or a hybrid cell
- A UE camped on a non-allowed CSG cell

A UE camped on an allowed CSG cell or a hybrid cell is in normal service. No special handling procedures are needed either on the network or the UE side since the UE is allowed access to the cell and can use the emergency services if available as on any other cell that supports these services.

In the idle mode procedures defined in TS 25.304 [4] and TS 36.304 [3], a CSG cell advertising a CSG ID not in the UE's Allowed CSG list or Operator CSG list is defined as an acceptable cell and a UE is allowed to camp on an acceptable cell in limited service if there is no other suitable cell available.

If the network supports emergency services for a UE in limited service, then the following special handling procedures apply:

- A UE in limited service is admitted at the non-allowed CSG cell regardless of the subscription information, i.e., CSG access control is not performed for a UE that performs the Attach procedure indicating emergency services.
- For a UE in normal service at a CSG cell whose CSG subscription has been removed or expired but the Allowed CSG list or Operator CSG list has not been updated, if the UE performs a Service Request at the CSG cell with active emergency bearers, the MME shall deactivate all non-emergency bearers and accept the Service Request.

Therefore, a UE requests emergency service, if available, at a CSG or a hybrid cell using the same procedures as it would at a non CSG cell based on whether the UE is in normal or limited service. No special UE procedures have been defined for initiating emergency services at a CSG cell.

NOTE: A UE only adds a CSG ID to the Allowed CSG list when it performs manual CSG selection as described in Section 5.4.2.2. Since emergency service does not require manual CSG selection, the UE does not update the Allowed CSG list if it is admitted at a CSG cell whose CSG is not present in the Allowed CSG list or the Operator CSG list.

On the network side, if the network supports emergency services for UEs in limited service, then the network will not perform CSG access control for that UE when the UE performs the attach procedure indicating emergency services.

9. Security procedures for the H(e)NB

9.1. General

The following security aspects need to be considered for deployment of H(e)NBs

1. Security architecture
2. Secuirty functions
   - Secure storage and execution
   - Mutual authentication
   - Location Verification

NOTE: This section provides a brief overview of the security aspects of H(e)NBs. For further details see TS 33.320 [10].

9.2. Security architecture reference model

The backhaul between a H(e)NB and operator's core network may be insecure. Therefore, a H(e)NB accesses the operator's core network via a Security Gateway (SeGW) by establishing a secure tunnel between the H(e)NB and the SeGW to protect information transmitted on the backhaul link.

Figure 9-1 describes the (E-)UTRAN security network architecture for H(e)NBs.

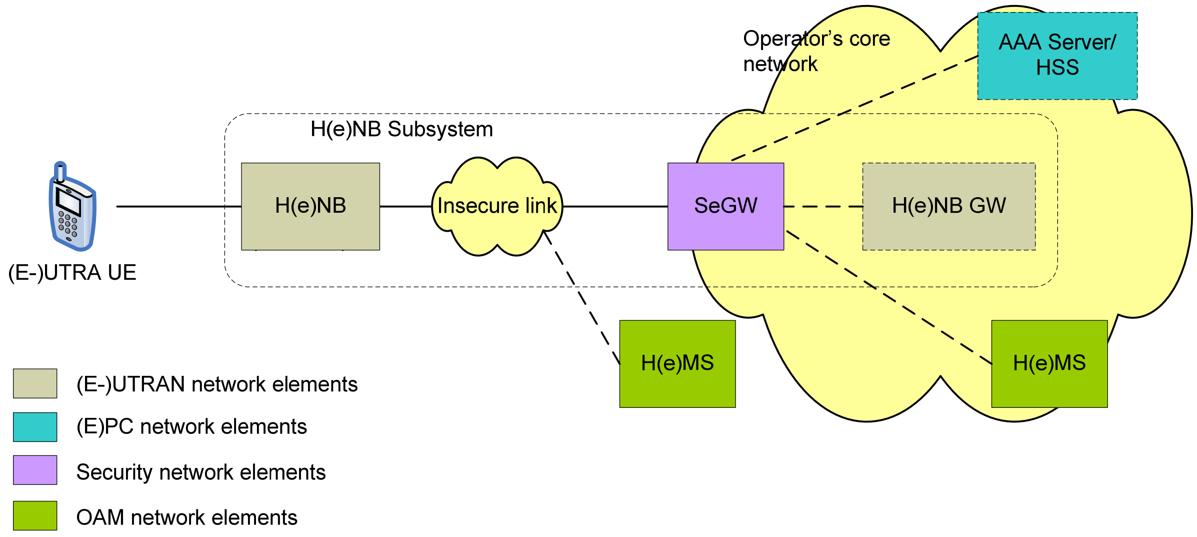

Figure 9-1: (E-)UTRAN security network architecture for H(e)NBs

The network elements that provide security functions include:

- **H(e)NB:** The backhaul link from the H(e)NB to the operator's core network is an insecure broadband connection. Therefore, IPSec is used to establish the security tunnel between the H(e)NB and the SeGW. IPSec is mandatory to implement but optional to use based on an operator policy.
- **SeGW:** The SeGW is at the border of the operator's core network. The SeGW represents the operator's core network to perform mutual authentication with the H(e)NB. After successful mutual authentication between the H(e)NB and the SeGW, the SeGW connects the H(e)NB to the operator's core network. Any connection between the H(e)NB and the core network is tunnelled through the SeGW.

NOTE: The SeGW and H(e)NB-GW are logically separate entities within the operator's network. If the SeGW and the H(e)NB-GW are not integrated, then the interface between them may be protected using NDS/IP [37]. In the absence of a HeNB-GW, the HeNB is directly connected to the MME via the SeGW.

- **HSS:** The HSS stores the subscription data and authentication information of the H(e)NBs. When hosting party authentication is required, the AAA server authenticates the hosting party based on the authentication information retrieved from the HSS. For further details see Section 9.3.
- **AAA server:** Optionally an AAA server may be used to verify the authorization of the H(e)NB to connect to the operator's network based on the authenticated device identity extracted from the H(e)NB certificate. This authorization check is separate from and in addition to the revocation status check via OCSP or CRL as defined in [38], [39] and [40]. In addition, when hosting party authentication is performed, the AAA server authenticates the hosting party based on the authentication information retrieved from HSS.
- **H(e)MS:** Secure communication is also required to H(e)NB Management System (H(e)MS). For a H(e)MS deployed behind the SeGW, the H(e)MS traffic may be protected by a TLS tunnel established between H(e)NB and H(e)MS. The H(e)MS may also be accessible on the public Internet. In this case the H(e)MS is exposed to attackers located in the insecure network and the H(e)MS traffic shall be protected by TLS tunnel established between H(e)NB and H(e)MS. In this case, mutual authentication between H(e)NB and H(e)MS shall be based on a device certificate for the H(e)NB and a network certificate for the H(e)MS.

9.3. Security functions

9.3.1. Secure storage and execution

Secure storage and execution consists of two elements defined in TS 33.320 [10]:

- **Hosting Party Module:** The Hosting Party Module (HPM) is a physical entity distinct from the H(e)NB physical equipment, dedicated to the identification and authentication of the Hosting Party towards the MNO. The HPM is provided by means of a UICC.

- **Trusted Environment:** The Trusted Environment (TrE) is a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. The TrE is used to perform the device integrity check upon booting and before connecting to the core network and/or to the H(e)MS.

9.3.2. Mutual authentication

There are two types of mutual authentication defined in TS 33.320 [10]:

- **Device mutual authentication**: The device mutual authentication is mandatory for the H(e)NB and performed between the H(e)NB and the SeGW using IKEv2 with certificates. On the H(e)NB the credentials and critical security functions for device authentication are protected inside a TrE.
    - All signalling, user, and management plane traffic over the interface between H(e)NB and SeGW is sent through the IPSec ESP tunnel (with NAT-T UDP encapsulation as necessary) that is established as a result of the device mutual authentication procedure.
- **Hosting party mutual authentication:** The hosting party mutual authentication is optionally performed by the operator’s network following successful device mutual authentication. The authentication of the hosting party uses an EAP/AKA method and is based on credentials contained in a separate Hosting Party Module (HPM) in H(e)NB, and in the MNO HLR/HSS.

9.3.3. Location verification

Operators require assurance of the H(e)NB location to satisfy various security, regulatory and operational requirements. The H(e)MS and/or H(e)NB-GW/MME perform location verification.

One or more of the following may be used to perform location verification:

- The public IP address of the broadband access device provided by the H(e)NB
- The IP address and/or access line location identifier provided by broadband access provider
- Information of macro-cells surrounding the H(e)NB provided by the H(e)NB
- Geo-coordinates provided by a GNSS receiver embedded into the H(e)NB

Different deployment scenarios and H(e)NB configurations will influence the availability, accuracy and reliability of these types of location information.

10. Operations, Administration, Maintenance and Provisioning (OAM&P) procedures for the H(e)NB

10.1. General

The following OAM aspects need to be considered for deployment of H(e)NBs

1. H(e)NB OAM functional architecture
2. OAM procedures
   - Discovery and registration
   - Configuration Management (CM), Fault management (FM) and Performance Management (PM) of H(e)NB

NOTE: This section provides a brief overview of the OAM functions for H(e)NBs. For further details see TS 32.583 [41] for HNBs and TS 32.593 [42] for HeNBs.

10.2. H(e)NB OAM functional architecture reference model

Figure 10-1 describes the (E-)UTRAN OAM functional architecture for H(e)NBs.

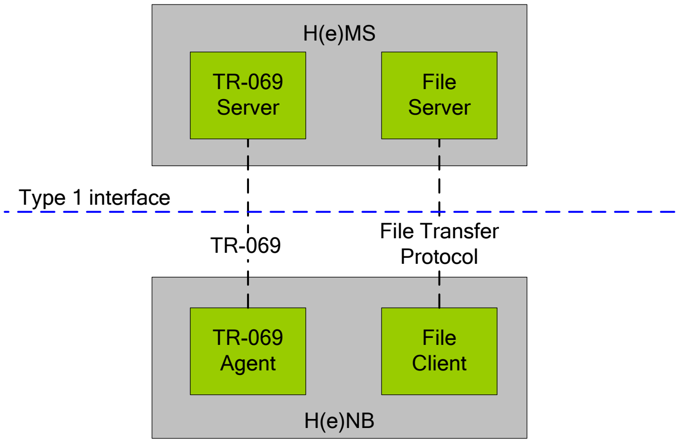

Figure 10-1: (E-)UTRAN OAM functional architecture for H(e)NBs

The network elements that provide OAM functions include:

- **H(e)MS:** The H(e)MS logically comprises a TR-069 Manager and a file server.
    - The TR-069 Manager corresponds to the TR-069 Auto-Configuration Server (ACS) function as defined in TR-069 specification [26].
    - The file server may be used for file upload or download related to H(e)MS management, such as upload of performance measurement files or alarm logs, as configured by TR-069 Manager. The file server may also be used for other purposes by network operator.
- **H(e)NB:** The H(e)NB logically comprises a TR-069 Agent and a file client.
    - The TR-069 Agent corresponds to the TR-069 Customer Premise Equipment (CPE) function as defined in TR-069 specification [26].
    - The file client may be used for file upload or download related to H(e)MS management, such as upload of performance measurement files or alarm logs, as configured by TR-069 Manager via TR-069 Agent. The file client may also be used for other purposes not related to H(e)NB management.

Typically, the H(e)MS assumes one of the following two roles:

- **Initial H(e)MS:** The Initial H(e)MS may be used to perform identity and location verification of H(e)NB and assign appropriate Serving H(e)MS, Security Gateway and H(e)NB-GW or MME to the H(e)NB. The FQDN of the Initial H(e)MS may be factory programmed in the H(e)NB.
- **Serving H(e)MS:** The Serving H(e)MS supports the procedures for CM/FM/PM, file upload/download, and identity verification of the H(e)NB. The Serving H(e)MS may also support H(e)NB-GW or MME discovery and assignment by H(e)NB. Typically, the Serving H(e)MS is located inside the operator's secure network domain and the address of the Serving H(e)MS is provided to the H(e)NB via the Initial H(e)MS.

NOTE: There may be an initial SeGW and a serving SeGW corresponding to the initial H(e)MS and the serving H(e)MS. For further details see TS 32.583 [41] and TS 32.593 [42]. The role of the SeGW in OAM is described in Section 9.

10.3. OAM procedures

10.3.1. Discovery and registration procedures

The discovery and registration procedures define the procedures for the assignment and establishment of connectivity of the H(e)NB to the Serving H(e)MS, the Serving SeGW, and the HNB-GW or the MME.

The H(e)NB needs to establish IP connectivity with the Serving H(e)MS for management purposes and with the H(e)NB-GW or MME for CS Core/(E)PC connectivity purposes when it is first powered up.

Two methods are defined for establishing IP connectivity with the Serving H(e)MS:

- Serving H(e)MS discovery via Initial H(e)MS accessible inside operator's private secure network domain
- Serving H(e)MS discovery via Initial H(e)MS accessible on the public internet

Once the H(e)NB has established the IP connectivity with the Serving H(e)MS, the H(e)NB must register with the Serving H(e)MS.

The IP address(es) of the Iuh/S1 interface is provided to the H(e)NB in one of the following ways:

- By the Initial H(e)MS during Serving H(e)MS discovery procedure
- By the Serving H(e)MS during the registration procedure of the H(e)NB with the H(e)MS.

The registration of the HNB with HNB-GW is specified in TS 25.467 [14] and of the HeNB with the HeNB-GW/MME in TS 36.413 [15].

10.3.2. Configuration management, fault management and performance management procedures

The following OAM procedures are defined for H(e)NBs using the TR-069 protocol specified in [26]:

10.3.2.1. Configuration management:-

Configuration management (CM) can be achieved either by means of TR-069 RPC methods as a mandatory feature or by means of file download as an optional feature.

- The RPC method uses the SetParameterValues RPC method to configure the parameters in the H(e)NB. The arguments include the list of parameters to be configured and their values.
- The file download occurs if the TR-069 Manager in the Serving H(e)MS triggers the H(e)NB to start a file download of configuration CM data following a registration of the H(e)NB with the Serving H(e)MS. Subsequent to this initial phase, the TR-069 Manager may trigger this procedure at any time.

CM capabilities support three different types of configuration parameters:

- Read-only parameters. These parameters are readable only by the H(e)MS.

- Read/Write parameters. In addition to read, the H(e)MS also has write access for these parameters, whereby the H(e)MS configures the value of the parameter. These parameters may have a default value specified.
- Auto-configurable parameters. This is a special case of read/write parameters. For these parameters, H(e)MS may configure a range from which H(e)NB selects a value using internal algorithms. The range can be as narrow as a single value (conventional Read/Write parameters) or can be as broad the full range available. Auto-configurable parameters provide the flexibility necessary for self-optimizing network (SON) framework, allowing the H(e)MS and H(e)NB to share the knowledge about the network that is useful for network optimization purposes. The support for auto-configurable parameters is indicated to the H(e)MS using read-only capability parameters.

10.3.2.2. Fault management:

Fault management (FM) uses the TR-069 Manager, using SetParameterValues method, to select alarm attributes (such as perceived severity, alarm type) that the H(e)NB shall use to classify its alarms for purpose of reporting them to TR-069 Manager. When an alarm occurs, the H(e)NB reports the alarm to the TR-069 Manager using the procedure that depends on the ReportingMechanism of the alarm defined

10.3.2.3. Performance management:

Performance management (PM) uses the TR-069 Manager, using SetParameterValues method, to set the PeriodicUploadInterval parameter to define the periodicity for PM file upload. The H(e)NB uploads the PM file to the File Server at every PeriodicUploadInterval. The upload method may be one of the following: FTP, SFTP, HTTP, or HTTPS.

11. Differentiated CSG charging

11.1. General

Procedures for charging at a CSG are defined TS 23.203 [43] to enable the following CSG specific charging models:

- Differentiated charging at a CSG cell
- Differentiated charging at a member hybrid cell
- Differentiated charging at a non-member hybrid cell

The CSG charging models are enabled by reporting the User CSG information to the appropriate network elements. The User CSG information includes CSG ID, access mode and CSG membership indication in the case of a hybrid cell.

11.2. User CSG Information reporting

As defined in TS 23.203 [43], for each of the different CSG charging models, if the reporting trigger is armed, then the GGSN should request the SGSN or the P-GW should request the S-GW (and then the SGSN or MME) to report any changes in user CSG information when the UE enters/leaves/accesses via a CSG cell or a hybrid cell corresponding to the trigger.

Upon the initial interaction with the PCEF, the PCRF may provide CSG information reporting triggers indicating how to set the CSG Information Reporting Action IE for User CSG Information reporting. If credit-authorization triggers and event triggers require different levels of reporting of User CSG information for a single UE, the User CSG information to be reported should be changed to the highest level of detail required.

NOTE: An operator should consider the increased core network signalling load generated by this type of reporting, and such reporting should be applied for a limited number of subscribers only.