3GPP TSG CT Meeting #28 **CP-050126**
1st – 3rd June 2005. Quebec, CANADA.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.008** **CR** **992** ⌘**rev** **-** ⌘ Current version: **6.8.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Modifications for PS HO in A/Gb mode
Source:	⌘	Infineon, Siemens
Work item code:	⌘	SCSAGB
Date:	⌘	10/05/2005
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	If the MS performs a RAU due to a PS handover in a new RA, it is clarified, that the transmission of UL data shall not be suspended. With the PS HO it is possible to assign new LLC and PFI values for a active NSAPI. The PS HO command may contain NAS specific information. This information is included in the 44.064 message PS HO command. It must be possible to indicate to the network whether the PS HO is supported.
Summary of change:	⌘	MS behaviour during a RAU triggered by a PS HO is introduced. The NAS container for PS HO is introduced.
Consequences if not approved:	⌘	Missing definition of the PS HO NAS container and the MS reaction upon reception of the container.

Clauses affected:	⌘	4.7.3.1.3; 4.7.5; 4.7.5.1.3; 4.7.5.1.4; 4.7.5.2.4; 4.7.7c (new); 6.1.3.3.5; 10.5.1.14 (new); 10.5.5.12; 10.5.5.12a

Other specs affected:	Y	N		
⌘	X		Other core specifications	⌘ 44.064 CR 011; 44.065 CR 023
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

4.7.3.1.3 GPRS attach accepted by the network

If the GPRS attach request is accepted by the network, an ATTACH ACCEPT message is sent to the MS.

The P-TMSI reallocation may be part of the GPRS attach procedure. When the ATTACH REQUEST includes the IMSI, the SGSN shall allocate the P-TMSI. The P-TMSI that shall be allocated is then included in the ATTACH ACCEPT message together with the routing area identifier. The network shall, in this case, change to state GMM-COMMON-PROCEDURE-INITIATED and shall start timer T3350 as described in subclause 4.7.6. Furthermore, the network may assign a P-TMSI signature for the GMM context which is then also included in the ATTACH ACCEPT message. If the LAI or PLMN identity that has been transmitted in the ATTACH ACCEPT message is a member of any of the "forbidden" lists, any such entry shall be deleted. Additionally, the network shall include the radio priority level to be used by the MS for mobile originated SMS transfer in the ATTACH ACCEPT message. In a shared network, the network shall indicate the PLMN identity of the CN operator that has accepted the GPRS attach request in the RAI contained in the ATTACH ACCEPT message (see 3GPP TS 23.251 [109]).

If the MS has indicated in the ATTACH REQUEST message that it supports PS inter-RAT handover to UTRAN Iu mode, the network may include in the ATTACH ACCEPT message a request to provide the Inter RAT information container.

In A/Gb mode, the Cell Notification information element shall be included in the ATTACH ACCEPT message by the network which indicates that the Cell Notification is supported by the network.

In Iu mode, the network should prolong the PS signalling connection if the mobile station has indicated a follow-on request pending in ATTACH REQUEST. The network may also prolong the PS signalling connection without any indication from the mobile terminal.

The MS, receiving an ATTACH ACCEPT message, stores the received routing area identification, stops timer T3310, reset the GPRS attach attempt counter, reset the routing area updating attempt counter, enters state GMM-REGISTERED and sets the GPRS update status to GU1 UPDATED.

If the message contains a P-TMSI, the MS shall use this P-TMSI as the new temporary identity for GPRS services. In this case, an ATTACH COMPLETE message is returned to the network. The MS shall delete its old P-TMSI and shall store the new one. If no P-TMSI has been included by the network in the ATTACH ACCEPT message, the old P-TMSI, if any available, shall be kept.

If the message contains a P-TMSI signature, the MS shall use this P-TMSI signature as the new temporary signature for the GMM context. The MS shall delete its old P-TMSI signature, if any is available, and shall store the new one. If the message contains no P-TMSI signature, the old P-TMSI signature, if available, shall be deleted.

If the network has requested the provision of the Inter RAT information container the MS shall return an ATTACH COMPLETE message including the Inter RAT information container IE to the network.

The network may also send a list of "equivalent PLMNs" in the ATTACH ACCEPT message. Each entry of the list contains a PLMN code (MCC+MNC). The mobile station shall store the list, as provided by the network, except that any PLMN code that is already in the "forbidden PLMN" list shall be removed from the "equivalent PLMNs" list before it is stored by the mobile station. In addition the mobile station shall add to the stored list the PLMN code of the registered PLMN that sent the list. All PLMNs in the stored list shall be regarded as equivalent to each other for PLMN selection, cell selection/re-selection and handover. The stored list in the mobile station shall be replaced on each occurrence of the ATTACH ACCEPT message. If no list is contained in the message, then the stored list in the mobile station shall be deleted. The list shall be stored in the mobile station while switched off so that it can be used for PLMN selection after switch on.

In Iu mode, if the network wishes to prolong the PS signalling connection (for example, if the mobile station has indicated "follow-on request pending" in ATTACH REQUEST message) the network shall indicate the "follow-on proceed" in the ATTACH ACCEPT message. If the network wishes to release the PS signalling connection, the network shall indicate "no follow-on proceed" in the ATTACH ACCEPT message.

After that in Iu mode, the mobile station shall act according to the follow-on proceed flag included in the Attach result information element in the ATTACH ACCEPT message (see subclause 4.7.13).

In A/Gb mode, if the ATTACH ACCEPT message contains the Cell Notification information element, then the MS shall start to use the LLC NULL frame to perform cell updates. The network receiving an ATTACH COMPLETE message stops timer T3350, changes to GMM-REGISTERED state and considers the P-TMSI sent in the ATTACH ACCEPT message as valid.

The network may also send a list of local emergency numbers in the ATTACH ACCEPT, by including the Emergency Number List IE. The mobile equipment shall store the list, as provided by the network, except that any emergency number that is already stored in the SIM/USIM shall be removed from the list before it is stored by the mobile equipment. If there are no emergency numbers stored on the SIM/USIM, then before storing the received list the mobile equipment shall remove from it any emergency number stored permanently in the ME for use in this case (see 3GPP TS 22.101 [8]). The list stored in the mobile equipment shall be replaced on each receipt of a new Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE are valid only in networks with the same MCC as in the cell on which this IE is received. If no list is contained in the ATTACH ACCEPT message, then the stored list in the mobile equipment shall be kept, except if the mobile equipment has successfully registered to a PLMN with an MCC different from that of the last registered PLMN.

The mobile equipment shall use the stored list of emergency numbers received from the network in addition to the emergency numbers stored on the SIM/USIM or ME to detect that the number dialled is an emergency number.

NOTE: The mobile equipment may use the emergency numbers list to assist the end user in determining whether the dialled number is intended for an emergency service or for another destination, e.g. a local directory service. The possible interactions with the end user are implementation specific.

The list of emergency numbers shall be deleted at switch off and removal of the SIM/USIM. The mobile equipment shall be able to store up to ten local emergency numbers received from the network.

4.7.5 Routing area updating procedure

This procedure is used for:

- normal routing area updating to update the registration of the actual routing area of an MS in the network. This procedure is used by GPRS MSs in MS operation mode C and by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS and non-GPRS services if the network operates in network operation mode II or III;

- combined routing area updating to update the registration of the actual routing and location area of an MS in the network. This procedure is used by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS and non-GPRS services provided that the network operates in network operation mode I;

- periodic routing area updating. This procedure is used by GPRS MSs in MS operation mode C and by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS or for GPRS and non-GPRS services independent of the network operation mode;

- IMSI attach for non-GPRS services when the MS is IMSI attached for GPRS services. This procedure is used by GPRS MSs in MS operation modes A or B, if the network operates in network operation mode I;

    - in A/Gb mode, resuming GPRS services when the RR sublayer indicated a resumption failure after dedicated mode was left, see 3GPP TS 44.018 [84];

    - in A/Gb mode, updating the network with the new MS Radio Access Capability IE when the content of the IE has changed;

    - updating the network with the new DRX parameter IE when the content of the IE has changed;

  NOTE 1: Such changes can be used e.g. when the MS activates a PDP context with service requirements that cannot be met with the current DRX parameter. As PDP context(s) are activated and deactivated, the GMM context will be updated with an appropriate DRX parameter;

- Iu mode to A/Gb mode and for A/Gb mode to Iu mode intersystem change, see subclause 4.7.1.7; or

- in Iu mode, to re-synchronize the PMM mode of MS and network after RRC connection release with cause "Directed signalling connection re-establishment", see subclause 4.7.2.5.

The routing area updating procedure shall also be used by a MS which is attached for GPRS services if a new PLMN is entered (see 3GPP TS 23.122 [14]).

Subclause 4.7.5.1 describes the routing area updating procedures for updating the routing area only. The combined routing area updating procedure used to update both the routing and location area is described in subclause 4.7.5.2.

The routing area updating procedure is always initiated by the MS. It is only invoked in state GMM-REGISTERED.

To limit the number of subsequently rejected routing area update attempts, a routing area updating attempt counter is introduced. The routing area updating attempt counter shall be incremented as specified in subclause 4.7.5.1.5. Depending on the value of the routing area updating attempt counter, specific actions shall be performed. The routing area updating attempt counter shall be reset when:

- a GPRS attach procedure is successfully completed; or

- a routing area updating procedure is successfully completed;

and additionally when the MS is in substate ATTEMPTING-TO-UPDATE:

- a new routing area is entered;

- expiry of timer T3302; or

- at request from registration function.

The mobile equipment shall contain a list of "forbidden location areas for roaming", as well as a list of "forbidden location areas for regional provision of service". The handling of these lists is described in subclause 4.4.1.

The Mobile Equipment shall contain a list of "equivalent PLMNs". The handling of this list is described in subclause 4.4.1.

In a shared network, the MS shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [14]. The MS shall construct the Routing Area Identification of the cell from this chosen PLMN identity, and the LAC and the RAC received on the BCCH. If the constructed RAI is different from the stored RAI, the MS shall initiate the routing area updating procedure. The chosen PLMN identity shall be indicated to the RAN in the RRC INITIAL DIRECT TRANSFER message (see 3GPP TS 25.331 [23c]). Whenever a ROUTING AREA UPDATING REJECT message with the cause "PLMN not allowed" is received by the MS, the chosen PLMN identity shall be stored in the "forbidden PLMN list". Whenever a ROUTING AREA UPDATING REJECT message is received by the MS with the cause "Roaming not allowed in this location area", "Location Area not allowed", or "No suitable cells in Location Area", the constructed RAI which triggered the routing area updating procedure shall be stored in the suitable list.

In A/Gb mode, user data transmission in the MS shall be suspended during the routing area updating procedure except if the routing area updating procedure is triggered by a PS Handover procedure as described in 3GPP TS 43.129 [113]; user data reception shall be possible. User data transmission in the network may be suspended during the routing area updating procedure.

In Iu mode, user data transmission and reception in the MS shall not be suspended during the routing area updating procedure. User data transmission in the network shall not be suspended during the routing area updating procedure.

In Iu mode, when a ROUTING AREA UPDATE REQUEST is received by the SGSN over a new PS signalling connection while there is an ongoing PS signalling connection (network is already in mode PMM-CONNECTED) for this UE, the network shall progress the routing area update procedure as normal and release the previous PS signalling connection when the routing area update procedure has been accepted by the network.

NOTE 2: The re-establishment of the radio bearers of active PDP contexts is done as described in subclause "Service Request procedure".

The network informs the MS about the support of specific features, such as LCS-MOLR, in the “Network feature support” Information Element. The information is either explicitly given by sending the “Network feature support” IE or implicitly by not sending it. The handling in the network is described in subclause 9.4.15.11. The MS may use the indication to inform the user about the availability of the appropriate services and it shall not request services that have not been indicated as available.

4.7.5.1.3 Normal and periodic routing area updating procedure accepted by the network

If the routing area updating request has been accepted by the network, a ROUTING AREA UPDATE ACCEPT message shall be sent to the MS. The network may assign a new P-TMSI and/or a new P-TMSI signature for the MS. If a new P-TMSI and/or P-TMSI signature have been assigned to the MS, it/they shall be included in the ROUTING AREA UPDATE ACCEPT message together with the routing area identification.In a shared network the network shall indicate the PLMN identity of the CN operator that has accepted the routing area updating request in the RAI contained in the ROUTING AREA UPDATE ACCEPT message (see 3GPP TS 23.251 [109]).

If a new DRX parameter was included in the ROUTING AREA UPDATE REQUEST message, the network shall store the new DRX parameter and use it for the downlink transfer of signalling and user data.

If the MS has indicated in the ROUTING AREA UPDATE REQUEST message that it supports PS inter-RAT handover to UTRAN Iu mode, the network may include in the ROUTING AREA UPDATE ACCEPT message a request to provide the Inter RAT information container.

In A/Gb mode the Cell Notification information element shall be included in the ROUTING AREA UPDATE ACCEPT message in order to indicate the ability of the network to support the Cell Notification.

The network shall change to state GMM-COMMON-PROCEDURE-INITIATED and shall start the supervision timer T3350 as described in subclause 4.7.6.

If the LAI or PLMN identity contained in the ROUTING AREA UPDATE ACCEPT message is a member of any of the "forbidden" lists then any such entry shall be deleted.

In Iu mode, the network should prolong the PS signalling connection if the mobile station has indicated a follow-on request pending in ROUTING AREA UPDATE REQUEST. The network may also prolong the PS signalling connection without any indication from the mobile terminal.

If the PDP context status information element is included in ROUTING AREA UPDATE REQUEST message, then the network shall deactivate all those PDP contexts locally (without peer to peer signalling between the MS and the network), which are not in SM state PDP-INACTIVE on network side but are indicated by the MS as being in state PDP-INACTIVE.

If the MBMS context status information element is included in the ROUTING AREA UPDATE REQUEST message, then the network shall deactivate all those MBMS contexts locally (without peer to peer signalling between the MS and network) which are not in SM state PDP-INACTIVE on the network side, but are indicated by the MS as being in state PDP-INACTIVE. If no MBMS context status information element is included, then the network shall deactivate all MBMS contexts locally which are not in SM state PDP-INACTIVE on the network side.

Upon receipt of a ROUTING AREA UPDATE ACCEPT message, the MS stores the received routing area identification, stops timer T3330, shall reset the routing area updating attempt counter and sets the GPRS update status to GU1 UPDATED. If the message contains a P-TMSI, the MS shall use this P-TMSI as new temporary identity for GPRS services and shall store the new P-TMSI. If no P-TMSI was included by the network in the ROUTING AREA UPDATING ACCEPT message, the old P-TMSI shall be kept. Furthermore, the MS shall store the P-TMSI signature if received in the ROUTING AREA UPDATING ACCEPT message. If no P-TMSI signature was included in the message, the old P-TMSI signature, if available, shall be deleted.

If the ROUTING AREA UPDATE REQUEST message was used to update the network with a new DRX parameter IE, the MS shall start using the new DRX parameter upon receipt of the ROUTING AREA UPDATE ACCEPT message.

If the PDP context status information element is included in ROUTING AREA UPDATE ACCEPT message, then the MS shall deactivate all those PDP contexts locally (without peer to peer signalling between the MS and network), which are not in SM state PDP-INACTIVE in the MS but are indicated by the network as being in state PDP-INACTIVE.

If the MBMS context status information element is included in the ROUTING AREA UPDATE ACCEPT message, then the MS shall deactivate all those MBMS contexts locally (without peer to peer signalling between the MS and network) which are not in SM state PDP-INACTIVE in the MS, but are indicated by the network as being in state PDP-INACTIVE. If no MBMS context status information element is included, then the MS shall deactivate all those MBMS contexts locally which are not in SM state PDP-INACTIVE in the MS.

In A/Gb mode, if the ROUTING AREA UPDATE ACCEPT message contains the Cell Notification information element, then the MS shall start to use the LLC NULL frame to perform cell updates.

The network may also send a list of "equivalent PLMNs" in the ROUTING AREA UPDATE ACCEPT message. Each entry of the list contains a PLMN code (MCC+MNC). The mobile station shall store the list, as provided by the network, except that any PLMN code that is already in the "forbidden PLMN" list shall be removed from the "equivalent PLMNs" list before it is stored by the mobile station. In addition the mobile station shall add to the stored list the PLMN code of the registered PLMN that sent the list. All PLMNs in the stored list shall be regarded as equivalent to each other for PLMN selection, cell selection/re-selection and handover. The stored list in the mobile station shall be replaced on each occurrence of the ROUTING AREA UPDATE ACCEPT message. If no list is contained in the message, then the stored list in the mobile station shall be deleted. The list shall be stored in the mobile station while switched off so that it can be used for PLMN selection after switch on.

A ROUTING AREA UPDATE COMPLETE message shall be returned to the network if the ROUTING AREA UPDATE ACCEPT message contained any of:

- a P-TMSI;
- Receive N-PDU Numbers (see 3GPP TS 44.065 [78] and 3GPP TS 25.322); or
- a request for the provision of the Inter RAT information container.

If Receive N-PDU Numbers were included, the Receive N-PDU Numbers values valid in the MS, shall be included in the ROUTING AREA UPDATE COMPLETE message.

If the network has requested the provision of the Inter RAT information container the MS shall return a ROUTING AREA UPDATE COMPLETE message including the Inter RAT information container IE to the network.

NOTE 1: In Iu mode, after a routing area updating procedure, the mobile station can initiate Service Request procedure to request the resource reservation for the active PDP contexts if the resources have been released by the network or send upper layer message (e.g. ACTIVATE PDP CONTEXT REQUEST) to the network via the existing PS signaling connection.

In Iu mode, if the network wishes to prolong the PS signalling connection (for example, if the mobile station has indicated "follow-on request pending" in ROUTING AREA UPDATE REQUEST message) the network shall indicate the "follow-on proceed" in the ROUTING AREA UPDATE ACCEPT message. If the network wishes to release the PS signalling connection, the network shall indicate "no follow-on proceed" in the ROUTING AREA UPDATE ACCEPT message.

After that in Iu mode, the mobile station shall act according to the follow-on proceed flag included in the Update result information element in the ROUTING AREA UPDATE ACCEPT message (see subclause 4.7.13).

The network may also send a list of local emergency numbers in the ROUTING AREA UPDATE ACCEPT, by including the Emergency Number List IE. The mobile equipment shall store the list, as provided by the network, except that any emergency number that is already stored in the SIM/USIM shall be removed from the list before it is stored by the mobile equipment. If there are no emergency numbers stored on the SIM/USIM, then before storing the received list the mobile equipment shall remove from it any emergency number stored permanently in the ME for use in this case (see 3GPP TS 22.101 [8]). The list stored in the mobile equipment shall be replaced on each receipt of a new Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE are valid only in networks with the same MCC as in the cell on which this IE is received. If no list is contained in the ROUTING AREA UPDATE ACCEPT message, then the stored list in the mobile equipment shall be kept, except if the mobile equipment has successfully registered to a PLMN with an MCC different from that of the last registered PLMN.

The mobile equipment shall use the stored list of emergency numbers received from the network in addition to the emergency numbers stored on the SIM/USIM or ME to detect that the number dialled is an emergency number.

NOTE 2: The mobile equipment may use the emergency numbers list to assist the end user in determining whether the dialled number is intended for an emergency service or for another destination, e.g. a local directory service. The possible interactions with the end user are implementation specific.

The list of emergency numbers shall be deleted at switch off and removal of the SIM/USIM. The mobile equipment shall be able to store up to ten local emergency numbers received from the network.

4.7.5.1.4 Normal and periodic routing area updating procedure not accepted by the network

If the routing area updating cannot be accepted, the network sends a ROUTING AREA UPDATE REJECT message to the MS. An MS that receives a ROUTING AREA UPDATE REJECT message, stops timer T3330, and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs". If a ROUTING AREA UPDATE REJECT message is received, the MS shall stop any ongoing transmission of user data.

The MS shall then take different actions depending on the received reject cause value:

3 (Illegal MS);

6 (Illegal ME);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and shall consider the SIM/USIM as invalid for GPRS services until switching off or the SIM/USIM is removed.

If the MS is IMSI attached, the MS shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid also for non-GPRS services until switching off or the SIM/USIM is removed.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2.9) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED.

If the update type is "periodic updating" a GPRS MS operating in MS operation mode A or B in networkoperation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

9 (MS identity cannot be derived by the network);

The MS shall set the GPRS update status to GU2 NOT UPDATED (and shall store it according to subclause 4.1.3.2), enter the state GMM-DEREGISTERED, and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. Subsequently, the MS may automatically initiate the GPRS attach procedure.

10 (Implicitly detached);

The MS shall change to state GMM-DEREGISTERED.NORMAL-SERVICE. The MS shall then perform a new attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP contexts.

NOTE: In some cases, user interaction may be required and then the MS cannot activate the PDP context(s) automatically.

11 (PLMN not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMN list".

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-DEREGISTERED.LIMITED-SERVICE.

The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304.

13 (Roaming not allowed in this location area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list. A GPRS MS operating in MS operation mode C shall perform a PLMN selection instead of a cell selection.

If the update type is "periodic updating" a GPRS MS operating in MS operation mode A or B in network operation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

A GPRS MS operating in MS operation mode A or B in network operation mode II or III, is still IMSI attached for CS services in the network.

15 (No Suitable Cells In Location Area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304.

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is described in subclause 4.7.5.1.5.

4.7.5.2.4 Combined routing area updating not accepted by the network

If the combined routing area updating cannot be accepted, the network sends a ROUTING AREA UPDATE REJECT message to the MS. An MS that receives a ROUTING AREA UPDATE REJECT message stops timer T3330, enters state MM IDLE, and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs". If a ROUTING AREA UPDATE REJECT message is received, the MS shall stop any ongoing transmission of user data.

The MS shall then take different actions depending on the received reject cause:

3 (Illegal MS);

6 (Illegal ME), or

8 (GPRS services and non GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and the update status to U3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, TMSI, RAI, LAI, ciphering key sequence number and GPRS ciphering key sequence number and shall consider the SIM/USIM as invalid for GPRS and non GPRS services until switching off or the SIM/USIM is removed.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED. If in the MS the timer T3212 is not already running, the timer shall be set to its initial value and restarted.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network. and shall then proceed with the appropriate MM specific procedure according to the MM service state.

9 (MS identity cannot be derived by the network);

The MS shall set the GPRS update status to GU2 NOT UPDATED (and shall store it according to subclause 4.1.3.2), enter the state GMM-DEREGISTERED, and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. Subsequently, the MS may automatically initiate the GPRS attach procedure.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network.

10 (Implicitly detached);

A GPRS MS operating in MS operation mode A or B in network operation mode I, is IMSI detached for both GPRS and CS services in the network.

The MS shall change to state GMM-DEREGISTERED.NORMAL-SERVICE. The MS shall then perform a new attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP context(s). The MS should also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE: In some cases, user interaction may be required and then the MS cannot activate the PDP/MBMS context(s) automatically.

11 (PLMN not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and the update status to U3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, TMSI, RAI, LAI, ciphering key sequence number GPRS ciphering key sequence number, and reset the location update attempt counter.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall then perform a PLMN selection according to 3GPP TS 23.122 [14].

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304.

13 (Roaming not allowed in this location area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED. If in the MS the timer T3212 is not already running, the timer shall be set to its initial value and restarted.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network and shall then proceed with the appropriate MM specific procedure according to the MM service state.

As an implementation option, a GPRS MS operating in operation mode A or B may perform a PLMN selection according to 3GPP TS 23.122 [14].

The MS shall not perform the optional PLMN selection in the case where the PLMN providing this reject cause is:

- On the "User Controlled PLMN Selector with Access Technology " or,
- On the "Operator Controlled PLMN Selector with Access Technology " list or,
- A PLMN identified as equivalent to any PLMN, with the same MCC, contained in the lists above.

15 (No Suitable Cells In Location Area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304.

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is described in subclause 4.7.5.2.5.

4.7.7 Authentication and ciphering procedure

4.7.7a Authentication and ciphering procedure used for UMTS authentication challenge.

The purpose of the authentication and ciphering procedure is fourfold (see 3GPP TS 33.102 [5a]):

- to permit the network to check whether the identity provided by the MS is acceptable or not;
- to provide parameters enabling the MS to calculate a new GPRS UMTS ciphering key and a new GPRS UMTS integrity key;
- to let the network set the GSM ciphering mode (ciphering /no ciphering) and GSM ciphering algorithm; and
- to permit the mobile station to authenticate the network.

In Iu mode, and in the case of a UMTS authentication challenge, the authentication and ciphering procedure can be used for authentication only.

The cases in which the authentication and ciphering procedure shall be used are defined in 3GPP TS 33.102 [5a] and 3GPP TS 42.009 [5].

The authentication and ciphering procedure is always initiated and controlled by the network. However, in the case of a UMTS authentication challenge, there is the possibility for the MS to reject the network.

The MS shall support the UMTS authentication challenge, if a USIM is inserted.

The authentication and ciphering procedure can be used for either:

- authentication only;
- setting of the GSM ciphering mode and the GSM ciphering algorithm only; or
- authentication and the setting of the GSM ciphering mode and the GSM ciphering algorithm.

In A/Gb mode, the network should not send any user data during the authentication and ciphering procedure.

A UMTS security context is established in the MS and the network when a UMTS authentication challenge is performed in A/Gb mode or in Iu mode. After a successful UMTS authentication, the GPRS UMTS ciphering key, the GPRS UMTS integrity key, the GPRS GSM ciphering key and the GPRS ciphering key sequence number, are stored both in the network and the MS.

4.7.7b Authentication and ciphering procedure used for GSM authentication challenge

The purpose of the authentication and ciphering procedure is threefold (see 3GPP TS 43.020 [13]):

- to permit the network to check whether the identity provided by the MS is acceptable or not;
- to provide parameters enabling the MS to calculate a new GPRS GSM ciphering key; and
- to let the network set the GSM ciphering mode (ciphering/no ciphering) and GSM ciphering algorithm.

The authentication and ciphering procedure can be used for either:

- authentication only;
- setting of the GSM ciphering mode and the GSM ciphering algorithm only; or
- authentication and the setting of the GSM ciphering mode and the GSM ciphering algorithm.

The cases in which the authentication and ciphering procedure shall be used are defined in 3GPP TS 42.009 [5].

In A/Gb mode, the authentication and ciphering procedure is always initiated and controlled by the network. It shall be performed in a non ciphered mode because of the following reasons:

- the network cannot decipher a ciphered AUTHENTICATION_AND_CIPHERING RESPONSE from an unauthorised MS and put it on the black list; and
- to be able to define a specific point in time from which on a new GPRS GSM ciphering key should be used instead of the old one.

GSM authentication challenge shall be supported by a ME supporting GERAN or UTRAN.

In A/Gb mode, the network should not send any user data during the authentication and ciphering procedure.

A GSM security context is established in the MS and the network when a GSM authentication challenge is performed in A/Gb mode or in Iu mode. However, in Iu mode the MS shall not accept a GSM authentication challenge, if a USIM is inserted. After a successful GSM authentication challenge, the GPRS GSM ciphering key and the GPRS ciphering key sequence number, are stored both in the network and the MS.

4.7.7c Change of the ciphering algorithm at PS Handover

For PS handover to A/Gb mode (see subclause 10.5.1.14 and 3GPP TS 44.060 [76]) the network shall either assign a GSM ciphering algorithm to be used in the target cell or deactivate ciphering in the target cell. The MS shall start to use the new GSM ciphering algorithm or deactivate ciphering upon an indication from the lower layers that the PS handover procedure has been successfully completed (see 3GPP TS 44.060 [76])

After PS handover to Iu mode (see 3GPP TS 25.331 [23c] and 3GPP TS 44.118 [111]) the network shall activate integrity protection and shall either assign a ciphering algorithm to be used in the target cell or deactivate ciphering in the target cell, using the security mode control procedure (3GPP TS 25.331 [23c] and 3GPP TS 44.118 [111]).

If the MS does not support the GSM ciphering algorithm indicated in the NAS container for PS HO information element, the MS shall skip the parameter when processing the information element and send an unciphered GMM STATUS message with cause #95 "semantically incorrect message".

6.1.3.1.1 Successful PDP context activation initiated by the mobile station

In order to request a PDP context activation, the MS sends an ACTIVATE PDP CONTEXT REQUEST message to the network, enters the state PDP-ACTIVE-PENDING and starts timer T3380. The message contains the selected NSAPI, PDP type, requested QoS and, if the MS requests a static address, the PDP address. The MS shall ensure that the selected NSAPI is not currently being used by another Session Management entity in the MS.

Upon receipt of an ACTIVATE PDP CONTEXT REQUEST message, the network selects a radio priority level based on the QoS negotiated and may reply with an ACTIVATE PDP CONTEXT ACCEPT message. Upon receipt of the message ACTIVATE PDP CONTEXT ACCEPT the MS shall stop timer T3380, shall enter the state PDP-ACTIVE. If the offered QoS parameters received from the network differ from the QoS requested by the MS, the MS shall either accept the negotiated QoS or initiate the PDP context deactivation procedure.

NOTE 1: If the MS requested a value for a QoS parameter that is not within the range specified by 3GPP TS 23.107, the network should negotiate the parameter to a value that lies within the specified range.

In A/Gb mode, the MS shall initiate establishment of the logical link for the LLC SAPI indicated by the network with the offered QoS and selected radio priority level if no logical link has been already established for that SAPI. If the offered QoS parameters received from the network differ from the QoS requested by the MS, the MS shall either accept the negotiated QoS or initiate the PDP context deactivation procedure. If the LLC SAPI indicated by the network can not be supported by the MS, the MS shall initiate the PDP context deactivation procedure.

In Iu mode, both the network and the MS shall store the LLC SAPI and the radio priority in the PDP context. If a Iu mode to A/Gb mode system change is performed, the new SGSN shall initiate establishment of the logical link using the negotiated QoS profile, the negotiated LLC SAPI, and selected radio priority level stored in the PDP context as in a A/Gb mode to A/Gb mode Routing Area Update.

An MS, which is capable of operating in both A/Gb mode and Iu mode, shall use a valid LLC SAPI, while an MS which is capable of operating only in Iu mode shall indicate the LLC SAPI value as "LLC SAPI not assigned" in order to avoid unnecessary value range checking and any other possible confusion in the network. When the MS uses a valid LLC SAPI, the network shall return a valid LLC SAPI. The network shall return the “LLC SAPI not assigned” value only when the MS uses the “LLC SAPI not assigned” value.

NOTE 2: The radio priority level and the LLC SAPI parameters, though not used in Iu mode, shall be included in the messages, in order to support handover between Iu mode and A/Gb mode networks.

6.1.3.3.1 Network initiated PDP Context Modification

In order to initiate the procedure, the network sends the MODIFY PDP CONTEXT REQUEST message to the MS and starts timer T3386. The message shall contain the new QoS and the radio priority level and LLC SAPI that shall be used by the MS in GSM at the lower layers for the transmission of data related to the PDP context.

Upon receipt of this message the MS shall reply with the MODIFY PDP CONTEXT ACCEPT message, if the MS accepts the new QoS and the indicated LLC SAPI.

If the MS does not accept the new QoS or the indicated LLC SAPI, the MS shall initiate the PDP context deactivation procedure for the PDP context - the reject cause IE value of the DEACTIVATE PDP CONTEXT REQUEST message shall indicate "QoS not accepted".

The network shall upon receipt of the MODIFY PDP CONTEXT ACCEPT message stop timer T3386.

In A/Gb mode, the network shall establish, reconfigure or continue using the logical link with the new QoS for the LLC SAPI indicated in the MODIFY PDP CONTEXT REQUEST message.

In Iu mode, the network shall establish, reconfigure or continue using the Radio Access Bearer with the new QoS indicated in the MODIFY PDP CONTEXT REQUEST message.

6.1.3.3.2 MS initiated PDP Context Modification accepted by the network

In order to initiate the procedure, the MS sends the MODIFY PDP CONTEXT REQUEST message to the network, enters the state PDP-MODIFY-PENDING and starts timer T3381. The message may contain the requested new QoS and/or the TFT and the requested LLC SAPI (used in A/Gb mode).

Upon receipt of the MODIFY PDP CONTEXT REQUEST message, the network may reply with the MODIFY PDP CONTEXT ACCEPT message in order to accept the context modification. The reply message may contain the negotiated QoS and the radio priority level based on the new QoS profile and the negotiated LLC SAPI, that shall be used in GSM by the logical link.

Upon receipt of the MODIFY PDP CONTEXT ACCEPT message, the MS shall stop the timer T3381. If the offered QoS parameters received from the network differs from the QoS requested by the MS, the MS shall either accept the negotiated QoS or initiate the PDP context deactivation procedure.

NOTE: When modification of QoS was requested by the MS, if the network does not accept the MS request, being unable to provide the requested QoS, it should maintain the QoS negotiated as previously negotiated or propose a new QoS. Therefore, the network would not reject the MS initiated PDP context modification request due to the unavailability of the required QoS. If the MS requested a value for a QoS parameter that is not within the range specified by 3GPP TS 23.107, the network should negotiate the parameter to a value that lies within the specified range.

6.1.3.3.3 MS initiated PDP Context Modification not accepted by the network

Upon receipt of a MODIFY PDP CONTEXT REQUEST message, the network may reject the MS initiated PDP context modification request by sending a MODIFY PDP CONTEXT REJECT message to the MS. The message shall contain a cause code that typically indicates one of the following:

26: insufficient resources;

32: Service option not supported;

41: semantic error in the TFT operation;

42: syntactical error in the TFT operation;

44: semantic errors in packet filter(s);

45: syntactical errors in packet filter(s);

95 - 111: protocol errors.

If upon the reception of a MODIFY PDP CONTEXT REQUEST message the network fails to re-establish the radio access bearer for a PDP context whose maximum bit rate in uplink and downlink is set to 0kbit/s, the network shall reply with MODIFY PDP CONTEXT REJECT with cause "insufficient resources".

The TFT in the request message is checked for different types of TFT IE errors as follows:

a) Semantic errors in TFT operations:

   1) *TFT operation* = "Create a new TFT" when there is already an existing TFT for the PDP context.

   2) When the *TFT operation* is an operation other than "Create a new TFT" and there is no TFT for the PDP context.

   3) *TFT operation* = "Delete existing TFT" when there is already another PDP context with the same PDP address and APN without a TFT.

   4) *TFT operation* = "Delete packet filters from existing TFT" when it would render the TFT empty.

   In these cases the network shall not diagnose an error and perform the following actions to resolve the inconsistency:

   In case 1) the network shall further process the new activation request and, if it was processed successfully, delete the old TFT.

   In case 2) the network shall:

   - further process the new request and, if no error according to list items b), c), and d) was detected, consider the TFT as successfully deleted, if the TFT operation is "Delete existing TFT" or "Delete packet filters from existing TFT";

   - process the new request as an activation request, if the TFT operation is "Add packet filters in existing TFT" or "Replace packet filters in existing TFT".

   In case 3) the network shall process the new deletion request and, after successful deletion of the TFT, deactivate the old PDP context with the same PDP address and APN without a TFT by explicit peer-to-peer signalling between the MS and the network.

   In case 4) the network shall further process the new request and, if no error according to list items b), c), and d) was detected, delete the existing TFT. After successful deletion of the TFT, if there was already another PDP context with the same PDP address and APN without a TFT, the network shall deactivate this old PDP context without a TFT by explicit peer-to-peer signalling between the MS and the network.

b) Syntactical errors in TFT operations:

   1) When the *TFT operation* is an operation other than "Delete existing TFT" and the packet filter list in the TFT IE is empty.

   2) *TFT operation* = "Delete existing TFT" with a non-empty packet filter list in the TFT IE.

   3) *TFT operation* = "Replace packet filters in existing TFT" when a to be replaced packet filter does not exist in the original TFT.

   4) *TFT operation* = "Delete packet filters from existing TFT" when a to be deleted packet filter does not exist in the original TFT.

   5) *TFT operation* = "Delete packet filters from existing TFT" with a packet filter list also including packet filters in addition to the packet filter identifiers.

   6) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list.

   In case 3) the network shall not diagnose an error, further process the replace request and, if no error according to list items c) and d) was detected, include the packet filters received to the existing TFT.

   In case 4) the network shall not diagnose an error, further process the deletion request and, if no error according to list items c) and d) was detected, consider the respective packet filter as successfully deleted.

Otherwise the network shall reject the modification request with cause "syntactical error in the TFT operation".

c) Semantic errors in packet filters:

When a packet filter consists of conflicting packet filter components which would render the packet filter ineffective, i.e. no IP packet will ever fit this packet filter. How the network determines a semantic error in a packet filter is outside the scope of the present document.

The network shall reject the modification request with cause "semantic errors in packet filter(s)".

d) Syntactical errors in packet filters:

1) When the *TFT operation* = "Create a new TFT" or "Add packet filters to existing TFT" and two or more packet filters in the resultant TFT would have identical packet filter identifiers.

2) When the *TFT operation* = "Create a new TFT" or "Add packet filters to existing TFT" or "Replace packet filters in existing TFT" and two or more packet filters in all TFTs associated with this PDP address and APN would have identical packet filter precedence values.

3) When there are other types of syntactical errors in the coding of packet filters, such as the use of a reserved value for a packet filter component identifier.

In case 1), if two or more packet filters with identical packet filter identifiers are contained in the new request, the network shall reject the modification request with cause "syntactical errors in packet filter(s)". Otherwise, the network shall not diagnose an error, further process the new request and, if it was processed successfully, delete the old packet filters which have the identical packet filter identifiers.

In case 2) the network shall not diagnose an error, further process the new request and, if it was processed successfully, delete the old packet filters which have identical filter precedence values. Furthermore, by means of explicit peer-to-peer signalling between the MS and the network, the network shall deactivate the PDP context(s) for which it has deleted the packet filters.

Otherwise the network shall reject the modification request with cause "syntactical errors in packet filter(s)".

Upon receipt of a MODIFY PDP CONTEXT REJECT message, the MS shall stop timer T3381 and enter the state PDP-ACTIVE.

6.1.3.3.4 Abnormal cases

a) Expiry of timers

On the network side:

On the first expiry of timer T3386, the network shall resend the MODIFY PDP CONTEXT REQUEST message reset and restart timer T3386. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3386, the network may continue to use the previously negotiated QoS or it may initiate the PDP context deactivation procedure.

In the MS:

On the first expiry of timer T3381, the MS shall resend the MODIFY PDP CONTEXT REQUEST message reset and restart timer T3381. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3381, the MS may continue to use the previously negotiated QoS or it may initiate the PDP context deactivation procedure.

b) Collision of MS and Network initiated PDP Context Modification Procedures

A collision of a MS and network initiated PDP context modification procedures is identified by the MS if a MODIFY PDP CONTEXT REQUEST message is received from the network after the MS has sent a MODIFY PDP CONTEXT REQUEST message itself, and both messages contain the same TI and the MS has not yet received a MODIFY PDP CONTEXT ACCEPT message from the network.

A collision is detected by the network in case a MODIFY PDP CONTEXT REQUEST message is received from the MS with the same TI as the MODIFY PDP CONTEXT REQUEST message sent to the MS.

In the case of such a collision, the network initiated PDP context modification shall take precedence over the MS initiated PDP context modification. The MS shall terminate internally the MS initiated PDP context modification procedure, enter the state PDP-Active and proceed with the network initiated PDP context modification procedure by sending a MODIFY PDP CONTEXT ACCEPT message. The network shall ignore the MODIFY PDP CONTEXT REQUEST message received in the state PDP-MODIFY-PENDING. The network shall proceed with the network initiated PDP context modification procedure as if no MODIFY PDP CONTEXT REQUEST message was received from the MS.

c) Collision of MS initiated PDP Context Modification Procedures and Network initiated Deactivate PDP Context Request Procedures

A collision of a MS initiated PDP context modification procedures and a network initiated PDP context deactivation procedures is identified by the MS if a DEACTIVATE PDP CONTEXT REQUEST message is received from the network after the MS has sent a MODIFY PDP CONTEXT REQUEST message, and the MS has not yet received a MODIFY PDP CONTEXT ACCEPT message from the network.

In the case of such a collision, the network initiated PDP context deactivation shall take precedence over the MS initiated PDP context modification. The MS shall terminate internally the MS initiated PDP context modification procedure, and proceed with the network initiated PDP context deactivation procedure by sending a DEACTIVATE PDP CONTEXT ACCEPT, enter the state PDP-INACTIVE. The network shall ignore the MODIFY PDP CONTEXT REQUEST message received in the state PDP-INACTIVE-PENDING. The network shall proceed with he network initiated PDP context deactivation procedure as if no MODIFY PDP CONTEXT REQUEST message was received from the MS.

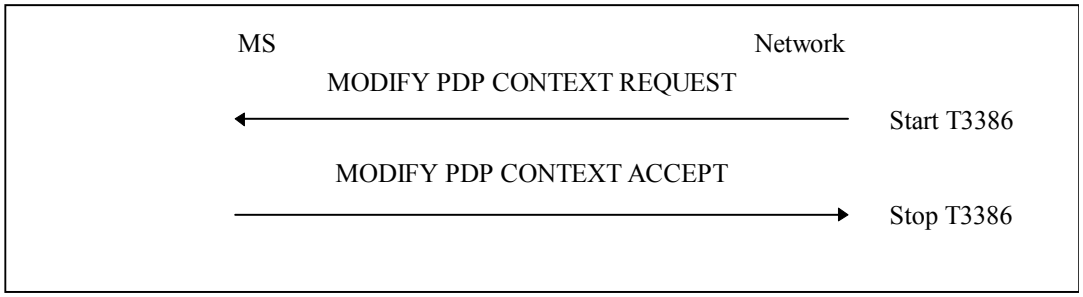

Figure 6.6/3GPP TS 24.008: Network initiated PDP context modification procedure

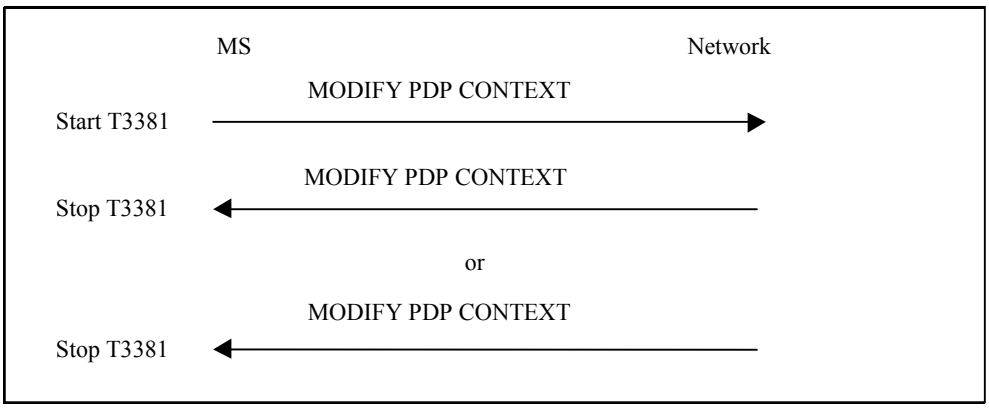

Figure 6.7/3GPP TS 24.008: MS initiated PDP context modification procedure

6.1.3.3.5 Modification of the NSAPI-SAPI-PFI mapping at PS Handover

For PS handover to A/Gb mode (see subclause 10.5.1.14 and 3GPP TS 44.060 [76]) the network may assign new LLC SAPI and PFI values for active PDP contexts to be used in the target cell. For PDP contexts whose NSAPI is not included in the NAS container for PS HO information element, the MS shall continue to use the same LLC SAPI and PFI values.

Upon indication from the lower layers that a PS handover procedure has been successfully completed (see 3GPP TS 44.060 [76]), if an indicated NSAPI does not correspond to an active PDP context or if the received NSAPI

value is "reserved", the MS shall skip the corresponding NSAPI-SAPI-PFI triplet without sending an SM STATUS message and continue to process the NAS container for PS HO information element.

NOTE: Any inconsistency between MS and network concerning the NSAPI values of active PDP contexts will be removed during the next routing area updating procedure.

Upon indication from the lower layers that a PS handover procedure has been successfully completed (see 3GPP TS 44.060 [76]), if any of the received SAPI or PFI values are "reserved", the MS shall skip the corresponding NSAPI-SAPI-PFI triplet when processing the NAS container for PS HO information element and shall send an SM STATUS message with cause #111 "protocol error, unspecified" using the transaction identifier corresponding to the NSAPI.

If the MS does not accept the indicated LLC SAPI for a certain PDP context, the MS shall initiate the PDP context deactivation procedure for the PDP context - the reject cause IE value of the DEACTIVATE PDP CONTEXT REQUEST message shall indicate "QoS not accepted".

10.5.1.14 NAS container for PS HO

The purpose of the *NAS container for PS HO* information element is to indicate the NAS specific information for the PS handover to A/Gb mode. The *NAS container for PS HO* information element is included in the PS HO command message, see 3GPP TS 44.060 [76]. The coding of the information element identifier and length information is defined in 3GPP TS 44.060 [76].

The content of the *NAS container for PS HO* information element is coded as shown in figure 10.5.1.14/3GPP TS 24.008 and table 10.5.1.14/3GPP TS 24.008. The minimum length of this information element is 5 octets, the maximum length is 28 octets. The MS shall ignore any additional octets received.

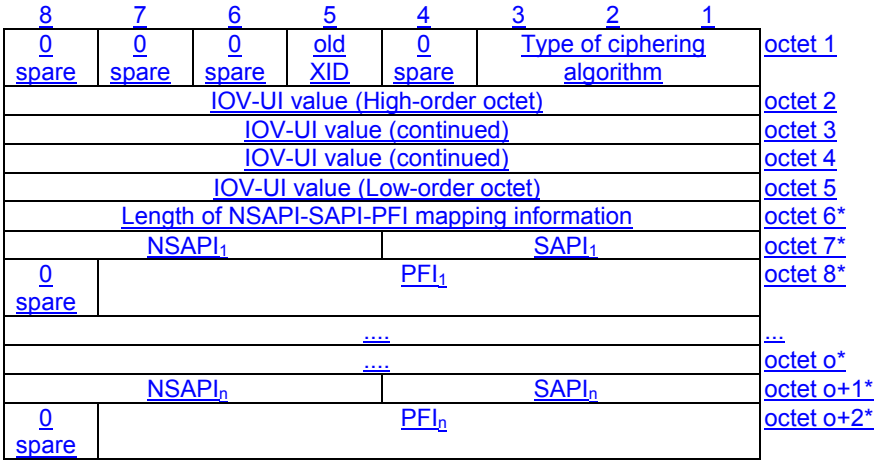

Figure 10.5.1.14/3GPP TS 24.008 *NAS container for PS HO* information element

Table 10.5.1.14/3GPP TS 24.008: *NAS container for PS HO* information element

Type of ciphering algorithm (octet 1, bits 1 to 3)
Bits

3	2	1	
0	0	0	ciphering not used
0	0	1	GPRS Encryption Algorithm GEA/1
0	1	0	GPRS Encryption Algorithm GEA/2
0	1	1	GPRS Encryption Algorithm GEA/3
1	0	0	GPRS Encryption Algorithm GEA/4
1	0	1	GPRS Encryption Algorithm GEA/5
1	1	0	GPRS Encryption Algorithm GEA/6
1	1	1	GPRS Encryption Algorithm GEA/7

Bit 4 of octet 1 is spare and shall be coded as zero.

old XID (octet 1, bit 5):
With this bit the network indicates, which LLC layer parameters and layer-3 parameters the MS shall use in the target cell after it has performed the Reset of LLC and SNDCP.

Bit 5
0 The MS shall perform the Reset of LLC and SNDCP and shall use the default configuration for the LLC layer parameters and layer-3 parameters.
1 The MS shall perform the Reset of LLC and SNDCP and shall re-initialize all LLC layer parameters and layer-3 parameters to the latest negotiated values (see 3GPP TS 44.064 [78a] and 3GPP TS 44.065 [78]).

If the old XID bit is set to 1, the network shall not include any NSAPI-SAPI-PFI mapping information in octet 8 and following octets and the MS shall ignore any NSAPI-SAPI-PFI mapping information given in octet 8 and following octets.

The bits 6 – 8 of octet 1 are spare and shall be coded all zeroes.

IOV-UI value (octet 2 to 5) The IOV-UI value consists of 32 bits, the format convention is defined in 3GPP TS 44.064 [78a]. **Length of NSAPI-SAPI-PFI mapping information** (octet 6) The Length of NSAPI-SAPI-PFI mapping information parameter indicates the number of octets of the subsequent NSAPI-SAPI-PFI mapping information. **NSAPI$_n$** (4 bit field): Network service access point identifier, coding see subclause 10.5.6.2.
SAPI$_n$ (4 bit field): LLC service access point identifier assigned to **NSAPI$_n$**, coding see subclause 10.5.6.9
PFI$_n$ (7 bit field): Packet Flow Identifier assigned to **NSAPI$_n$**, coding see subclause 10.5.6.11

10.5.5.12 MS network capability

The purpose of the *MS network capability* information element is to provide the network with information concerning aspects of the mobile station related to GPRS. The contents might affect the manner in which the network handles the operation of the mobile station. The *MS network capability* information indicates general mobile station characteristics and it shall therefore, except for fields explicitly indicated, be independent of the frequency band of the channel it is sent on.

The *MS network capability* is a type 4 information element with a maximum of 10 octets length.

The value part of a *MS network capability*information element is coded as shown in figure 10.5.128/3GPP TS 24.008 and table 10.5.145/3GPP TS 24.008.

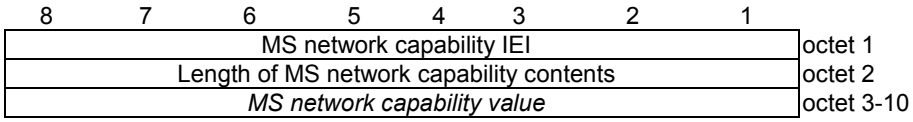

Figure 10.5.128/3GPP TS 24.008 MS network capability information element

Table 10.5.145/3GPP TS 24.008 *MS network capability* information element

<MS network capability value part> ::=

<**GEA1 bits**>
<**SM capabilities via dedicated channels**: bit>
<**SM capabilities via GPRS channels**: bit>
<**UCS2 support**: bit>
<**SS Screening Indicator**: bit string(2)>
<SoLSA Capability : bit>
<Revision level indicator: bit>
<PFC feature mode: bit>
<Extended GEA bits>
< LCS VA capability: bit >
< PS inter-RAT HO to UTRAN Iu mode capability: bit >
<Spare bits>;

<GEA1 bits> ::= **< GEA/1** :bit>;

<Extended GEA bits> ::= <GEA/2:bit><GEA/3:bit>< GEA/4:bit >< GEA/5:bit >< GEA/6:bit ><GEA/7:bit>;

<**Spare bits**> ::= null | {<spare bit> < **Spare bits** >};

SS Screening Indicator
0 0 defined in 3GPP TS 24.080

0 1 defined in 3GPP TS 24.080
1 0 defined in 3GPP TS 24.080
1 1 defined in 3GPP TS 24.080

SM capabilities via dedicated channels
0 Mobile station does not support mobile terminated point to point SMS via CS domain
1 Mobile station supports mobile terminated point to point SMS via CS domain

SM capabilities via GPRS channels
0 Mobile station does not support mobile terminated point to point SMS via PS domain
1 Mobile station supports mobile terminated point to point SMS via PS domain

UCS2 support
This information field indicates the likely treatment by the mobile station of UCS2 encoded character strings.
0 the ME has a preference for the default alphabet (defined in 3GPP TS 23.038 [8b]) over UCS2.
1 the ME has no preference between the use of the default alphabet and the use of UCS2.

GPRS Encryption Algorithm GEA/1
0 encryption algorithm **GEA/1**not available
1 encryption algorithm **GEA/1** available

SoLSA Capability
0 The ME does not support SoLSA.
1 The ME supports SoLSA.

Revision level indicator
0 used by a mobile station not supporting R99 or later versions of the protocol
1 used by a mobile station supporting R99 or later versions of the protocol

PFC feature mode
0 Mobile station does not support BSS packet flow procedures
1 Mobile station does support BSS packet flow procedures

GEA/2
0 encryption algorithm GEA/2 not available

1 encryption algorithm GEA/2 available

GEA/3
0 encryption algorithm GEA/3 not available
1 encryption algorithm GEA/3 available

GEA/4
0 encryption algorithm GEA/4 not available
1 encryption algorithm GEA/4 available

GEA/5
0 encryption algorithm GEA/5 not available
1 encryption algorithm GEA/5 available

GEA/6
0 encryption algorithm GEA/6 not available
1 encryption algorithm GEA/6 available

GEA/7
0 encryption algorithm GEA/7 not available
1 encryption algorithm GEA/7 available

LCS VA capability (LCS value added location request notification capability)
This information field indicates the support of the LCS value added location request notification via PS domain as defined in 3GPP TS 23.271 [105].
0 location request notification via PS domain not supported
1 location request notification via PS domain supported

PS inter-RAT HO to UTRAN Iu mode capability
This information field indicates the support of the PS inter-RAT HO to UTRAN Iu mode.
0 PS inter-RAT HO to UTRAN Iu mode not supported
1 PS inter-RAT HO to UTRAN Iu mode supported

10.5.5.12a MS Radio Access capability

The purpose of the *MS RA capability* information element is to provide the radio part of the network with information concerning radio aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station.

The *MS RA capability* is a type 4 information element, with a maximum length of 52 octets.

The value part of a *MS RA capability* information element is coded a shown table 10.5.146/3GPP TS 24.008.

For the indication of the radio access capabilities the following conditions shall apply:

- Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.
- Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile station should provide the relevant radio access capability for either GSM 1800 band OR GSM 1900 band, not both.
- The MS shall indicate its supported Access Technology Types during a single MM procedure.
- If the alternative coding by using the Additional access technologies struct is chosen by the mobile station, the mobile station shall indicate its radio access capability for the serving BCCH frequency band in the first included Access capabilities struct, if this information element is not sent in response to an Access Technologies Request from the network or if none of the requested Access Technology Types is supported by the MS. Otherwise, the mobile station shall include the radio access capabilities for the frequency bands it supports in the order of priority requested by the network (see 3GPP TS 44.060).
- The first Access Technology Type shall not be set to "1111".

For error handling the following shall apply:

– If a received Access Technology Type is unknown to the receiver, it shall ignore all the corresponding fields.

– If within a known Access Technology Type a receiver recognizes an unknown field it shall ignore it.

– For more details about error handling of MS radio access capability see 3GPP TS 48.018 [86].

Table 10.5.146/3GPP TS 24.008: *Mobile Station Radio Access Capability* Information Element

<MS RA capability value part> : < MS RA capability value part struct >>
<spare bits>**; -- *may be used for future enhancements*

<MS RA capability value part struct >::= --*recursive structure allows any number of Access technologies*
{ { < **Access Technology Type**: bit (4) > exclude 1111
< **Access capabilities** : <Access capabilities struct> > }

| { < **Access Technology Type**: bit (4) == 1111 > -- *structure adding Access technologies with same capabilities*
< **Length** : bit (7) > -- *length in bits of list of Additional access technologies and spare bits*
{ 1 < **Additional access technologies**: < Additional access technologies struct > > } ** 0
<spare bits>** } }

{ 0 | 1 <MS RA capability value part struct> } ;

< Additional access technologies struct > ::=
< **Access Technology Type** : bit (4) >
< **GMSK Power Class** : bit (3) >
< **8PSK Power Class** : bit (2) > ;

< Access capabilities struct > ::=
< **Length** : bit (7) > -- length in bits of Content and spare bits
<Access capabilities : <Content>>
<spare bits>** ; -- expands to the indicated length
-- may be used for future enhancements

< Content > ::=
< **RF Power Capability** : bit (3) >
{ 0 | 1 <**A5 bits** : <A5 bits> > } -- *zero means that the same values apply for parameters as in the immediately preceding Access capabilities field within this IE*
< **ES IND** : bit >
< **PS** : bit >
< **VGCS** : bit >
< **VBS** : bit >
{ 0 | 1 < **Multislot capability** : Multislot capability struct > } -- *zero means that the same values for multislot parameters as given in an earlier Access capabilities field within this IE apply also here*
-- *Additions in release 99*
{ 0 | 1 < **8PSK Power Capability** : bit(2) >} -- *'1' also means 8PSK modulation capability in uplink.*
< **COMPACT Interference Measurement Capability : bit >**
< **Revision Level Indicator** : bit >
< **UMTS FDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **UMTS 3.84 Mcps TDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **CDMA 2000 Radio Access Technology Capability** : bit > -- *3G RAT*
-- *Additions in release 4*
< **UMTS 1.28 Mcps TDD Radio Access Technology Capability**: bit > -- *3G RAT*
< **GERAN Feature Package 1** : bit >
{ 0 | 1 < **Extended DTM GPRS Multi Slot Class** : bit(2) >
< **Extended DTM EGPRS Multi Slot Class** : bit(2) > }
< Modulation based multislot class support : bit >
-- *Additions in release 5*
{ 0 | 1 < **High Multislot Capability** : bit(2) > }
{ 0 | 1 < **GERAN Iu Mode Capabilities** > } -- *'1' also means support of GERAN Iu mode*
< **GMSK Multislot Power Profile** : bit (2) >
< **8-PSK Multislot Power Profile** : bit (2) >
-- *Additions in release 6*
< **Multiple TBF Capability** : bit >
< **Downlink Advanced Receiver Performance** : bit(2) >
< **Extended RLC/MAC Control Message Segmentation Capability** : bit >
< **DTM Enhancements Capability** : bit >
< **PS Handover Capability** : bit >;

```
-- error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology
```

Table 10.5.146/3GPP TS 24.008 (continued): *Mobile Station Radio Access Capability* IE

< Multislot capability struct > ::=
{ 0 | 1 < **HSCSD multislot class** : bit (5) > }
{ 0 | 1 < **GPRS multislot class** : bit (5) > < **GPRS Extended Dynamic Allocation Capability** : bit > }
{ 0 | 1 < **SMS_VALUE** : bit (4) > < **SM_VALUE** : bit (4) > }
-- *Additions in release 99*
{ 0 | 1 < **ECSD multislot class** : bit (5) > }
{ 0 | 1 < **EGPRS multislot class** : bit (5) > < **EGPRS Extended Dynamic Allocation Capability** : bit > }
{0 | 1 < **DTM GPRS Multi Slot Class**: bit(2)>
<Single Slot DTM : bit>
{0 | 1 <**DTM EGPRS Multi Slot Class** : bit(2)> } } ;
-- error: struct too short, assume features do not exist

< **GERAN Iu Mode Capabilities** > ::=
< **Length** : bit (4) > -- *length in bits of Iu mode-only capabilities and spare bits*
-- *Additions in release 6*
< **FLO Iu Capability** : bit >
<spare bits>** ; -- *expands to the indicated length*
-- *may be used for future enhancements*

<A5 bits> ::= < A5/1 : bit> <A5/2 : bit> <A5/3 : bit> <A5/4 : bit> <A5/5 : bit> <A5/6 : bit> <A5/7 : bit>; -- bits for circuit mode ciphering algorithms. These fields are not used by the network and may be excluded by the MS.

Access Technology Type
This field indicates the access technology type to be associated with the following access capabilities.

Bits
4 3 2 1
0 0 0 0 GSM P
0 0 0 1 GSM E --*note that GSM E covers GSM P*
0 0 1 0 GSM R --*note that GSM R covers GSM E and GSM P*
0 0 1 1 GSM 1800
0 1 0 0 GSM 1900
0 1 0 1 GSM 450
0 1 1 0 GSM 480
0 1 1 1 GSM 850
1 0 0 0 GSM 700
1 0 0 1 GSM T 380
1 0 1 0 GSM T 410
1 0 1 1 GSM T 900
1 1 1 1 Indicates the presence of a list of Additional access technologies
All other values are treated as unknown by the receiver.

A MS which does not support any GSM access technology type shall set this field to '0000'.

RF Power Capability, GMSK Power Class (3 bit field)
This field contains the binary coding of the power class used for GMSK associated with the indicated Access Technology Type (see 3GPP TS 45.005).

A MS which does not support any GSM access technology type shall set this field to '000'.

8PSK Power Capability (2 bit field)
If 8-PSK modulation is supported for uplink, this field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005 [33]):
Bits 2 1
0 0 Reserved
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

8PSK Power Class (2 bit field)
This field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005):
Bits 2 1
0 0 8PSK modulation not supported for uplink
0 1 Power class E1
1 0 Power class E2

1 1 Power class E3

Additional access technologies struct
This structure contains the GMSK Power Class and 8PSK Power Class for an additional Access Technology. All other capabilities for this indicated Access Technology are the same as the capabilities indicated by the preceding Access capabilities struct.

A5/1
0 encryption algorithm A5/1 not available
1 encryption algorithm A5/1 available
A5/2
0 encryption algorithm A5/2 not available
1 encryption algorithm A5/2 available
A5/3
0 encryption algorithm A5/3 not available
1 encryption algorithm A5/3 available
A5/4
0 encryption algorithm A5/4 not available
1 encryption algorithm A5/4 available
A5/5
0 encryption algorithm A5/5 not available
1 encryption algorithm A5/5 available
A5/6
0 encryption algorithm A5/6 not available
1 encryption algorithm A5/6 available
A5/7
0 encryption algorithm A5/7 not available
1 encryption algorithm A5/7 available

ES IND – (Controlled early Classmark Sending)
0 "controlled early Classmark Sending" option is not implemented
1 "controlled early Classmark Sending" option is implemented

Table 10.5.146/3GPP TS 24.008 (concluded): *Mobile Station Radio Access Capability* IE

PS – (Pseudo Synchronisation)
0 PS capability not present
1 PS capability present

VGCS – (Voice Group Call Service)
0 no VGCS capability or no notifications wanted
1 VGCS capability and notifications wanted.

VBS – (Voice Broadcast Service)
0 no VBS capability or no notifications wanted
1 VBS capability and notifications wanted

HSCSD Multi Slot Class
The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

GPRS Multi Slot Class
The GPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

ECSD Multi Slot Class
The presence of this field indicates ECSD capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

EGPRS Multi Slot Class
The presence of this field indicates EGPRS capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The EGPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

GPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for GPRS is not implemented
1 Extended Dynamic Allocation Capability for GPRS is implemented

EGPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for EGPRS is not implemented
1 Extended Dynamic Allocation Capability for EGPRS is implemented

SMS_VALUE (Switch-Measure-Switch) (4 bit field)
The SMS field indicates the time needed for the mobile station to switch from one radio channel to another, perform a neighbor cell power measurement, and the switch from that radio channel to another radio channel. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)

(SM_VALUE) Switch-Measure (4 bit field)
The SM field indicates the time needed for the mobile station to switch from one radio channel to another and perform a neighbour cell power measurement. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)

DTM GPRS Multi Slot Class (2 bit field)
This field indicates the DTM GPRS multislot capabilities of the MS. It is coded as follows:
Bits
2 1
0 0 Unused. If received, the network shall interpret this as '01'
0 1 Multislot class 5 supported
1 0 Multislot class 9 supported
1 1 Multislot class 11 supported

Single Slot DTM (1 bit field)
This field indicates whether the MS supports single slot DTM operation (see 3GPP TS 43.055 [87]).
Bit
0 Single Slot DTM not supported
1 Single Slot DTM supported

An MS indicating support for Extended DTM GPRS multislot class or Extended DTM EGPRS multislot class shall set this bit to '1'. The network may ignore the bit in this case.

DTM EGPRS Multi Slot Class (2 bit field)
This field indicates the DTM EGPRS multislot capabilities of the MS. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS multislot Class field.

COMPACT Interference Measurement Capability (1 bit field)
0 COMPACT Interference Measurement Capability is not implemented
1 COMPACT Interference Measurement Capability is implemented

Revision Level Indicator (1 bit field)
Bit
0 The ME is Release '98 or older
1 The ME is Release '99 onwards

UMTS FDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS FDD not supported
1 UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 3.84 Mcps TDD not supported
1 UMTS 3.84 Mcps TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)
Bit
0 CDMA 2000 not supported
1 CDMA 2000 supported

UMTS 1.28 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 1.28 Mcps TDD not supported
1 UMTS 1.28 Mcps TDD supported

GERAN Feature Package 1 (1 bit field)
This field indicates whether the MS supports the GERAN Feature Package 1 (see 3GPP TS 44.060). It is coded as follows:

0 GERAN feature package 1 not supported.
1 GERAN feature package 1 supported.

Extended DTM GPRS Multi Slot Class (2 bit field)
This field indicates the extended DTM GPRS capabilities of the MS and shall be interpreted in conjunction with the DTM GPRS Multi Slot Class field. It is coded as follows, where 'DGMSC' denotes the DTM GPRS multislot class field:

DGMSC Bit	2 1	**Bit 2 1**	
	0 0	**0 0**	Unused. If received, it shall be interpreted as '01 00'
	0 0	**0 1**	Unused. If received, it shall be interpreted as '01 00'
	0 0	**1 0**	Unused. If received, it shall be interpreted as '01 00'
	0 0	**1 1**	Unused. If received, it shall be interpreted as '01 00'
	0 1	**0 0**	Multislot class 5 supported

0 1	**0 1**	Multislot class 6 supported
0 1	**1 0**	Unused. If received, it shall be interpreted as ‘01 00’
0 1	**1 1**	Unused. If received, it shall be interpreted as ‘01 00’
1 0	**0 0**	Multislot class 9 supported
1 0	**0 1**	Multislot class 10 supported
1 0	**1 0**	Unused. If received, it shall be interpreted as ’10 00’
1 0	**1 1**	Unused. If received, it shall be interpreted as ’10 00’
1 1	**0 0**	Multislot class 11 supported
1 1	**0 1**	Unused. If received, it shall be interpreted as ’11 00’
1 1	**1 0**	Unused. If received, it shall be interpreted as ’11 00’
1 1	**1 1**	Unused. If received, it shall be interpreted as ’11 00’

The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink. When this field is not present, the MS supports the multislot class indicated by the *DTM GPRS Multi Slot Class* field.

Extended DTM EGPRS Multislot Class (2 bit field)
This field is not considered when the DTM EGPRS Multislot Class field is not included. This field indicates the extended DTM EGPRS multislot capabilities of the MS and shall be interpreted in conjunction with the DTM EGPRS Multislot Class field. This field is coded as the Extended DTM GPRS Multislot Class field. The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink. When this field is not present, the MS supports the multislot class indicated by the DTM EGPRS Multi Slot Class field.

Modulation based multislot class support (1 bit field)
Bit
0 "Modulation based multislot class" not supported
1 "Modulation based multislot class" supported

High Multislot Capability (2 bit field)
The High Multislot Capability is individually combined with each multislot class field sent by the MS (the possible multislot class fields are: HSCSD multislot class, ECSD multislot class, GPRS multislot class, EGPRS multislot class, DTM GPRS multislot class, DTM EGPRS multislot class, extended DTM GPRS multislot class and extended DTM EGPRS multislot class) to extend the related multislot class to multislot classes 30 to 45, see 3GPP TS 45.002.
For each multislot class, the following mapping is done:
Bits

2 1	coded multislot class field	actual multislot class
0 0	8	30
0 0	10, 23, 28, 29	39
0 0	11, 20, 25	32
0 0	12, 21, 22, 26, 27	33
0 0	Any other	Multislot Class field value
0 1	8	35
0 1	10, 19, 24	36
0 1	11, 23, 28, 29	45
0 1	12, 21, 22, 26, 27	38
0 1	Any other	Multislot Class field value
1 0	8	40
1 0	10, 19, 24	41
1 0	11, 20, 25	42
1 0	12, 23, 28, 29	44
1 0	Any other	Multislot Class field value
1 1	12, 21, 22, 26, 27	43
1 1	11, 20, 25	37
1 1	10, 19, 24	31
1 1	9, 23, 28, 29	34
1 1	Any other	Multislot Class field value

GERAN Iu Mode Capabilities
This field indicates if the mobile station supports GERAN Iu mode. Furthermore, it indicates the GERAN Iu mode capabilities of the mobile station. The field shall be included if the mobile station supports GERAN Iu mode. If the field is not present, the mobile station does not support GERAN Iu mode.

FLO Iu Capability (1 bit field)
If this parameter is not present, the value '0' shall be assumed by the receiver.
0 FLO in GERAN Iu mode not supported
1 FLO in GERAN Iu mode supported

GMSK Multislot Power Profile (2 bit field)
For detailed definitions, see the Mobile Station Classmark 3 information element.

8-PSK Multislot Power Profile (2 bit field)
For detailed definitions, see the Mobile Station Classmark 3 information element.

Multiple TBF Capability (1 bit field)
Bit
0 Multiple TBF procedures in A/Gb mode not supported
1 Multiple TBF procedures in A/Gb mode supported

Downlink Advanced Receiver Performance (2 bit field)
This field indicates Downlink Advanced Receiver Performance capabilities of the MS (see 3GPP TS 45.005).
Bits
2 1
0 0 Downlink Advanced Receiver Performance not supported
0 1 Downlink Advanced Receiver Performance – phase I supported
Other values shall not be used by the MS.
If other values are received by the network, they shall be interpreted as '01'.

Extended RLC/MAC Control Message Segmentation capability (1 bit field)
Bit
0 Extended RLC/MAC control message segmentation not supported
1 Extended RLC/MAC control message segmentation supported

DTM Enhancements Capability (1 bit field)
This field indicates whether the mobile station supports enhanced DTM CS establishment and enhanced DTM CS release or not. It is coded as follows:
Bit
0 The mobile station does not support enhanced DTM CS establishment and enhanced DTM CS release procedures.
1 The mobile station supports enhanced DTM CS establishment and enhanced DTM CS release procedures.

PS Handover Capability (1 bit field)
This field indicates whether the mobile station supports the PS Handover. The PS Handover Capability applies to all RATs and modes indicated as supported in this information element.
Bit
0 The mobile station does not support the PS Handover.
1 The mobile station supports the PS Handover

*** next section for information only ***

10.5.5.3 Ciphering algorithm

The purpose of the *ciphering algorithm* information element is to specify which ciphering algorithm shall be used.

The *ciphering algorithm* is a type 1 information element.

The *ciphering algorithm* information element is coded as shown in figure 10.5.119/3GPP TS 24.008 and table 10.5.136/3GPP TS 24.008.

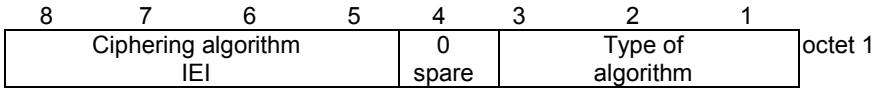

Figure 10.5.119/3GPP TS 24.008: *Ciphering algorithm* information element

Table 10.5.136/3GPP TS 24.008: *Ciphering algorithm* information element

Type of ciphering algorithm (octet 1)			
Bits			
3	**2**	**1**	
0	0	0	ciphering not used
0	0	1	GPRS Encryption Algorithm GEA/1
0	1	0	GPRS Encryption Algorithm GEA/2
0	1	1	GPRS Encryption Algorithm GEA/3
1	0	0	GPRS Encryption Algorithm GEA/4
1	0	1	GPRS Encryption Algorithm GEA/5
1	1	0	GPRS Encryption Algorithm GEA/6
1	1	1	GPRS Encryption Algorithm GEA/7

10.5.6.2 Network service access point identifier

The purpose of the *network service access point identifier* information element is to identify the service access point that is used for the GPRS data transfer at layer 3.

The *network service access point identifier* is a type 3 information element with a length of 2 octets.

The value part of a *network service access point identifier* information element is coded as shown in figure 10.5.135/3GPP TS 24.008 and table 10.5.153/3GPP TS 24.008.

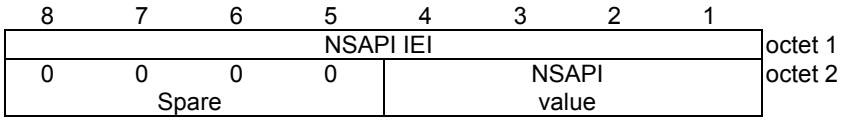

Figure 10.5.135/3GPP TS 24.008: *Network service access point identifier* information element

Table 10.5.153/3GPP TS 24.008: *Network service access point identifier* information element

NSAPI value (octet 2)

Bits 4	3	2	1	
0	0	0	0	reserved
0	0	0	1	reserved
0	0	1	0	reserved
0	0	1	1	reserved
0	1	0	0	reserved
0	1	0	1	NSAPI 5
0	1	1	0	NSAPI 6
0	1	1	1	NSAPI 7
1	0	0	0	NSAPI 8
1	0	0	1	NSAPI 9
1	0	1	0	NSAPI 10
1	0	1	1	NSAPI 11
1	1	0	0	NSAPI 12
1	1	0	1	NSAPI 13
1	1	1	0	NSAPI 14
1	1	1	1	NSAPI 15

10.5.6.9 LLC service access point identifier

The purpose of the *LLC service access point identifier* information element is to identify the service access point that is used for the GPRS data transfer at LLC layer.

The *LLC service access point identifier* is a type 3 information element with a length of 2 octets.

The value part of a *LLC service access point identifier* information element is coded as shown in figure 10.5.141/3GPP TS 24.008 and table 10.5.159/3GPP TS 24.008.

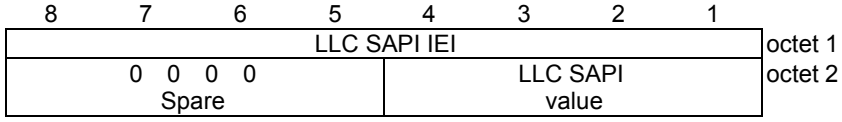

Figure 10.5.141/3GPP TS 24.008: *LLC service access point identifier* information element

Table 10.5.159/3GPP TS 24.008: *LLC service access point identifier* information element

LLC SAPI value (octet 2) Bit **4 3 2 1** 0 0 0 0 LLC SAPI not assigned 0 0 1 1 SAPI 3 0 1 0 1 SAPI 5 1 0 0 1 SAPI 9 1 0 1 1 SAPI 11 All other values are reserved.

10.5.6.11 Packet Flow Identifier

The *Packet Flow Identifier (PFI)* information element indicates the Packet Flow Identifier for a Packet Flow Context.

The *Packet Flow Identifier* is a a type 4 information element with 3 octets length.

The *Packet Flow Identifier* information element is coded as shown in figure 10.5.143/3GPP TS 24.008 and table 10.5.161/3GPP TS 24.008.

8	7	6	5	4	3	2	1	
Packet Flow Identifier IEI								octet 1
Length of Packet Flow Identifier IE								octet 2
Spare 0				Packet Flow Identifier value				octet 3

Figure 10.5.143/3GPP TS 24.008: *Packet Flow Identifier* information element

Table 10.5.161/3GPP TS 24.008: *Packet Flow Identifier* information element

Packet Flow Identifier value (octet 3) Bits **7 6 5 4 3 2 1** 0 0 0 0 0 0 0 Best Effort 0 0 0 0 0 0 1 Signaling 0 0 0 0 0 1 0 SMS 0 0 0 0 0 1 1 TOM8 0 0 0 0 1 0 0 } to } reserved 0 0 0 0 1 1 1 } 0 0 0 1 0 0 0 } to } dynamically assigned 1 1 1 1 1 1 1 }