3GPP TSG_CN#6 **NP-99451**
ETSI SMG3 Plenary Meeting #6,
Nice, France
13th – 15th December 1999

Agenda item: **5.1.3**

Source: **TSG_N WG1**

Title: **CRs on Work Item Security**

Introduction:

This document contains **"1"** CR agreed by **TSG_N WG1** and forwarded to **TSG_N Plenary** meeting **#6** for approval.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N1-99E95	24.008	042	4	C	R99	3.1.0	3.2.0	Adaptation of MM and GMM messages to incorporate UMTS security parameters

3GPP/SMG Meeting #9
Bad Aibling, Germany, 30 Nov-3 Dec 1999

Document* *N1-99E95
Revision of N1-99E14

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

24.008	**CR**	**042r4**	Current Version:	3.1.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ ↑ *CR number as allocated by MCC support team*

For submission to:	TSG N #6	for approval	☒	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM □ ME ☒ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: Vodafone **Date:** 23-11-1999

Subject: Adaptation of MM and GMM messages to incorporate UMTS security parameters

Work item: Security- 2G/3G interoperability

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	☒		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change:

UMTS authentication and ciphering mechanisms differ slightly to those used by GSM/GPRS. At the moment, in CN1 it has been agreed to use MM and GMM messages in UMTS. However, there are currently no messages defined to authenticate the user or negotiate ciphering keys etc. This CR proposes, that as an extension to the way GSM/GPRS handles these procedures, MM and GMM messages should be enhanced to include authentication and ciphering for UMTS.

The advantages of this proposed solution are:

- Backwards compatability with GSM/GPRS.
- Allows a GSM SIM to be used in a UMTS terminal
- Allows for future releases to enhance security mechanisms, as it keeps transparency in the terminal and in the HLR.
- Respects the 20 octet maximum of the layer 3 messages.

Clauses affected:

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

4.1.2.3 MM sublayer states on the network side

1. IDLE

The MM sublayer is not active except possibly when the RR sublayer is in Group Receive mode.

2. WAIT FOR RR CONNECTION

The MM sublayer has received a request for MM connection establishment from the CM layer. A RR connection to the mobile station is requested from the RR sublayer (i.e. paging is performed).

3. MM CONNECTION ACTIVE

The MM sublayer has a RR connection to a mobile station. One or more MM connections are active.

4. IDENTIFICATION INITIATED

The identification procedure has been started by the network. The timer T3270 is running.

5. AUTHENTICATION INITIATED

The authentication procedure has been started by the network. The timer T3260 is running.

6. TMSI REALLOCATION INITIATED

The TMSI reallocation procedure has been started by the network. The timer T3250 is running.

7. ~~CIPHERING~~SECURITY MODE INITIATED

The ~~cipher~~security mode setting procedure has been requested to the RR sublayer.

8a. WAIT FOR MOBILE ORIGINATED MM CONNECTION

A CM SERVICE REQUEST message is received and processed, and the MM sublayer awaits the "opening message" of the MM connection.

8b. WAIT FOR NETWORK ORIGINATED MM CONNECTION

A CM SERVICE PROMPT message has been sent by the network and the MM sublayer awaits the “opening message” of the MM connection $(CCBS)$.

9. WAIT FOR REESTABLISHMENT

The RR connection to a mobile station with one or more active MM connection has been lost. The network awaits a possible re-establishment request from the mobile station.

10. WAIT OF A GROUP CALL

Only applicable in case for mobile station supporting VGCS talking. The MM sublayer has received a request for establishing a VGCS from the GCC sublayer. The request for establishing a VGCS channels is given to the RR sublayer.

11. GROUP CALL ACTIVE

Only applicable in case of mobile station supporting VGCS talking. A VGCS channel is established by the RR sublayer. An RR connection to the talking mobile station can be established by the RR sublayer on the VGCS channel. The MM sublayer is active but no sending of MM message between the network and the mobile station has occurred.

12. MM CONNECTION ACTIVE (GROUP CALL)

    Only applicable in case of mobile station supporting VGCS talking. The MM sublayer has a RR connection to the talking mobile station on the VGCS channel. Only one MM connection is active.

13. WAIT FOR BROADCAST CALL

    Only applicable in case of VBS. The MM sublayer has received a request for a VBS establishment from the BCC sublayer. The request for establishment of VBS channels is given to the RR sublayer.

14. BROADCAST CALL ACTIVE

    Only applicable in case of VBS. A VBS channel is established by the RR sublayer. The MM sublayer is active but no explicit MM establishment between the Network and the mobile station has occurred.

4.3.2 Authentication procedure

4.3.2a Authentication procedure used for a UMTS authentication challenge

The purpose of the authentication procedure is fourfold:

First to permit the network to check whether the identity provided by the mobile station is acceptable or not (see GSM 03.20);

Second to provide parameters enabling the mobile station to calculate a new ciphering key.

Third to provide parameters enabling the mobile station to calculate a new integrity key.

Fourth to permit the receiving entity to check the integrity of the network.

The cases where the authentication procedure should be used are defined in GSM 02.09.
The authentication 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.

4.3.2b Authentication Procedure used for a GSM authentication challenge

The purpose of the authentication procedure is twofold:

First to permit the network to check whether the identity provided by the mobile station is acceptable or not (see GSM 03.20);

Second to provide parameters enabling the mobile station to calculate a new ciphering key.

The cases where the authentication procedure should be used are defined in GSM 02.09.
The authentication procedure is always initiated and controlled by the network.

4.3.2.1 Authentication request by the network

The network initiates the authentication procedure by transferring an AUTHENTICATION REQUEST message across the radio interface and starts the timer T3260. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see GSM 03.20 (GSM) and TS 33.102 (UMTS)). It also contains the ciphering key sequence number allocated to the key(s) which may be computed from the given parameters.

4.3.2.2 Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. It shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network. The new ciphering key (GSM authentication challenge) or the new ciphering key and the new integrity key (UMTS authentication challenge) calculated from the challenge information shall overwrite the previous one(s) and be stored on the SIM before the AUTHENTICATION RESPONSE message is transmitted. The ciphering key(s) stored in the SIM shall be loaded in to the ME when any valid ~~CIPHERING~~SECURITY MODE COMMAND is received during an RR connection (the definition of a valid ~~CIPHERING~~SECURITY MODE COMMAND message is given in GSM 04.18 section 3.4.7.2 (GSM) or in TS 25.331 (UMTS)). The ciphering key sequence number shall be stored together with the calculated key(s).

The SIM will provide the mobile station with the authentication response, based upon the authentication challenge from the network. For example, a UMTS authentication challenge will result in the SIM passing a RES, a Ciphering Key and an Integrity Key to the mobile station. A GSM authentication challenge will result in the SIM passing a SRES and a Ciphering Key to the mobile station.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20).

4.3.2.4 Ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets.~~, i.e. f~~In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter~~SRES~~ and the ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter and the ciphering key and the integrity key can be computed given the secret key associated to the IMSI.

In order to allow start of ciphering on a RR connection without authentication, the ciphering key sequence numbers are introduced. The sequence number is managed by the network in the way that the AUTHENTICATION REQUEST message contains the sequence number allocated to the key(s) which may be computed from the RAND parameter carried in that message.
The mobile station stores this number with the key(s), and indicates to the network in the first message (LOCATION UPDATING REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST) which sequence number the stored key or set of keys has. When the deletion of the sequence number is described this also means that the associated key(s) shall be considered as invalid.
The network may choose to start ciphering with the stored key(s) (under the restrictions given in GSM 02.09) if the stored sequence number and the one given from the mobile station are equal.

4.3.2.5 ~~Unsuccessful a~~Authentication not accepted by the network

If authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.
If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.
After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in section 3.5 of 04.18 (GSM) or in TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U2 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.
If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow section 4.3.4.3.
If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.
A R99 GSM-only MS connected to a R99 core network (even using the BSS radio access) shall support a UMTS authentication challenge.
Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see TS 33.102). This parameter contains two possible causes for authentication failure:

(a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a CS AUTHENTICATION FAILURE message (9.2.3a) to the network, with the failure cause 'CS MAC failure' (see 33.102). Thereafter the procedural behaviour is ffs.

(b) SQN failure

If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a CS AUTHENTICATION FAILURE message (9.2.3a) to the network, with the failure cause 'CS Synch failure' and parameters provided by the SIM (see 33.102) Upon receipt of this message, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

Note: Actions might vary according to the presence/absence of an integrity protected connection to a different core network node.

4.3.2.6 Abnormal cases

(a) RR connection failure:

Upon detection of a RR connection failure before the AUTHENTICATION RESPONSE is received, the network shall release all MM connections (if any) and abort any ongoing MM specific procedure.

(b) Expiry of timer T3260:

The authentication procedure is supervised on the network side by the timer T3260. At expiry of this timer the network may release the RR connection. In this case the network shall abort the authentication procedure and any ongoing MM specific procedure, release all MM connections if any, and initiate the RR connection release procedure described in section 3.5.

```
mobile station                          network
                  AUT REQ
            <------------------         Start T3260
                  AUT RES
             ------------------>       Stop T3260
                    (a)
                  AUT REJ
            < - - - - - - - - - -
                    (b)
```

Figure 4.2/TS 24.008: Authentication sequence: (a) authentication; (b) authentication rejection.

4.3.5.2 Abort procedure in the mobile station

At the receipt of the ABORT message the mobile station shall abort any MM connection establishment or call re-establishment procedure and release all MM connections (if any). If cause value #6 is received the mobile station shall delete any TMSI, LAI and ciphering key sequence number stored in the SIM, set the update status to ROAMING NOT ALLOWED (and store it in the SIM according to section 4.1.2.2) and consider the SIM invalid until switch off or the SIM is removed. As a consequence the mobile station enters state MM IDLE, substate NO IMSI after the release of the RR connection.

The mobile station shall then wait for the network to release the RR connection - see section 4.5.3.1.

4.4.2 Periodic updating

Periodic updating may be used to notify periodically the availability of the mobile station to the network. Periodic updating is performed by using the location updating procedure. The location updating type information element in the LOCATION UPDATING REQUEST message shall indicate periodic updating.

The procedure is controlled by the timer T3212 in the mobile station. If the timer is not already started, the timer is started each time the mobile station enters the MM IDLE substate NORMAL SERVICE or ATTEMPTing TO UPDATE. When the MS leaves the MM Idle State the timer T3212 shall continue running until explicitly stopped.

The timer is stopped (shall be set to its initial value for the next start) when:

- a LOCATION UPDATING ACCEPT or LOCATION UPDATING REJECT message is received;
- an AUTHENTICATION REJECT message is received;
- the first MM message is received, or ~~ciphering~~security mode setting is completed in the case of MM connection establishment, except when the most recent service state is LIMITED SERVICE;
- the mobile station has responded to paging and thereafter has received the first correct layer 3 message except RR message;
- the mobile station is deactivated (i.e. equipment powered down or SIM removed).

When the timer T3212 expires, the location updating procedure is started and the timer shall be set to its initial value for the next start. If the mobile station is in other state than MM Idle when the timer expires the location updating procedure is delayed until the MM Idle State is entered.

The conditions under which the periodic location updating procedure is used by a mobile station in the MM IDLE state are defined for each service state in section 4.2.2.

If the mobile station is in service state NO CELL AVAILABLE, LIMITED SERVICE, PLMN SEARCH or PLMN SEARCH-NORMAL SERVICE when the timer expires the location updating procedure is delayed until this service state is left. The (periodic) location updating procedure is not started if the BCCH information at the time the procedure is triggered indicates that periodic location shall not be used. The timeout value is broadcasted in the SYSTEM INFORMATION TYPE 3 message on the BCCH, in the Control channel description IE, see section 10.5.2.11.

The T3212 timeout value shall not be changed in the NO CELL AVAILABLE, LIMITED SERVICE, PLMN SEARCH and PLMN SEARCH-NORMAL SERVICE states.

When a change of the T3212 timeout value has to be taken into account and the timer is running (at change of the serving cell or, change of the broadcast value of T3212), the MS shall behave as follows:

Let t1 be the new T3212 timeout value and let t be the current timer value at the moment of the change to the new T3212 timeout value; then the timer shall be restarted with the value t modulo t1.

When the mobile station is activated, or when a change of the T3212 timeout value has to be taken into account and the timer is not running, the mobile station shall behave as follows:

Let t1 be the new T3212 timeout value, the new timer shall be started at a value randomly, uniformly drawn between 0 and t1.

4.4.4.4 ~~Ciphering~~Security mode setting by the network

The ~~ciphering~~security mode setting procedure (see section 3.4.7) may be initiated by the network, e.g., if a new TMSI has to be allocated.

4.4.4.7 Location updating not accepted by the network

If the location updating cannot be accepted the network sends a LOCATION UPDATING REJECT message to the mobile station. The mobile station receiving a LOCATION UPDATING REJECT message shall stop the timer T3210, store the reject cause, start T3240, enter state LOCATION UPDATING REJECTED await the release of the RR connection triggered by the network. Upon the release of the RR connection the mobile station shall take the following actions depending on the stored reject cause:

# 2: IMSI unknown in HLR;

# 3: Illegal MS; or

# 6: Illegal ME.

The mobile station shall set the update status to ROAMING NOT ALLOWED (and store it in the SIM according to section 4.1.2.2), and delete any TMSI, stored LAI and ciphering key sequence number and shall consider the SIM as invalid until switch-off or the SIM is removed.

# 11: PLMN not allowed;

# 12: Location Area not allowed; or

# 13: Roaming not allowed in this location area.

The mobile station shall delete any LAI, TMSI and ciphering key sequence number stored in the SIM, reset the attempt counter, set the update status to ROAMING NOT ALLOWED (and store it in the SIM according to section 4.1.2.2). The mobile station shall store the LAI or the PLMN identity in the suitable forbidden list, i.e. in the "forbidden PLMN list" for cause #11, in the list of "forbidden location areas for regional provision of service" for cause #12, and in the list of "forbidden location areas for roaming" for cause #13. In addition, the MS will memorize if cause #13 was received, so to perform a PLMN selection instead of a cell selection when back to the MM IDLE state.

Other values are considered as abnormal cases and the specification of the mobile station behaviour in those cases is given in section 4.4.4.9.

4.4.4.9 Abnormal cases on the mobile station side

The different abnormal cases that can be identified are the following:

a) Access barred because of access class control

The location updating procedure is not started. The mobile station stays in the current serving cell and applies normal cell reselection process. The procedure is started as soon as possible and if still necessary (when the barred state is ended or because of a cell change)

b) The answer to random access is an IMMEDIATE ASSIGNMENT REJECT message

The location updating is not started. The mobile station stays in the chosen cell and applies normal cell selection process. The waiting timer T3122 is reset when a cell change occurs. The procedure is started as soon as possible after T3122 timeout if still necessary.

c) Random access failure

Timer T3213 is started. When it expires the procedure is attempted again if still necessary.

NOTE: As specified in GSM 05.08, a cell reselection then takes place, with return to the cell inhibited for 5 seconds if there is at least one other suitable cell. Typically the selection process will take the mobile station back to the cell where the random access failed after 5 seconds.

If at the expiry of timer T3213 a new cell has not been selected due to the lack of valid information (see GSM 05.08), the mobile station may as an option delay the repeated attempt for up to 8 seconds to allow cell re-selection to take place. In this case the procedure is attempted as soon as a new cell has been selected or the mobile station has concluded that no other cell can be selected.

If random access failure occurs for two successive random access attempts for location updating the mobile station proceeds as specified below.

d) RR connection failure

The procedure is aborted and the mobile station proceeds as specified below.

e) T3210 timeout

The procedure is aborted, the RR connection is aborted and the MS proceeds as specified below.

f) RR release before the normal end of procedure

The procedure is aborted and the mobile station proceeds as specified below.

g) Location updating reject, other causes than those treated in section 4.4.4.7

The MS waits for release of the RR connection as specified in section 4.4.4.8, and then proceeds as specified below.

In cases d) to g) above and for repeated failures as defined in c) above the mobile station proceeds as follows. Timer T3210 is stopped if still running. The RR Connection is aborted in case of timer T3210 timeout. The attempt counter is incremented. The next actions depend on the Location Area Identities (stored and received from the BCCH of the current serving cell) and the value of the attempt counter.

– the update status is UPDATED, and the stored LAI is equal to the one received on the BCCH from the current serving cell and the attempt counter is smaller than 4:

  The mobile station shall keep the update status to UPDATED, the MM IDLE sub-state after the RR connection release is NORMAL SERVICE. The mobile station shall memorize the location updating type used in the location updating procedure. It shall start timer T3211 when the RR connection is released. When timer T3211 expires the location updating procedure is triggered again with the memorized location updating type;

– either the update status is different from UPDATED, or the stored LAI is different from the one received on the BCCH from the current serving cell, or the attempt counter is greater or equal to 4:

  The mobile station shall delete any LAI, TMSI, ciphering key sequence number stored in the SIM, set the update status to NOT UPDATED and enter the MM IDLE sub-state ATTEMPTING TO UPDATE when the RR connection is released (See section 4.2.2.2 for the subsequent actions). If the attempt counter is smaller than 4, the mobile station shall memorize that timer T3211 is to be started when the RR connection is released, otherwise it shall memorize that timer T3212 is to be started when the RR connection is released.

4.5.1.1 MM connection establishment initiated by the mobile station

Upon request of a CM entity to establish an MM connection the MM sublayer first decides whether to accept, delay, or reject this request:

- An MM connection establishment may only be initiated by the mobile station when the following conditions are fulfilled:

  - Its update status is UPDATED.

  - The MM sublayer is in one of the states MM IDLE or MM connection active but not in MM connection active (Group call).

  An exception from this general rule exists for emergency calls (see section 4.5.1.5). A further exception is defined in the following clause.

- If an MM specific procedure is running at the time the request from the CM sublayer is received, and the LOCATION UPDATING REQUEST message has been sent, the request will either be rejected or delayed, depending on implementation, until the MM specific procedure is finished and, provided that the network has not sent a "follow-on proceed" indication, the RR connection is released. If the LOCATION UPDATING REQUEST message has not been sent, the mobile station may include a "follow-on request" indicator in the message. The mobile station shall then delay the request until the MM specific procedure is completed, when it may be given the opportunity by the network to use the RR connection: see section 4.4.4.6.

In order to establish an MM connection, the mobile station proceeds as follows:

a) If no RR connection exists, the MM sublayer requests the RR sublayer to establish an RR connection and enters MM sublayer state WAIT FOR RR CONNECTION (MM CONNECTION). This request contains an establishment cause and a CM SERVICE REQUEST or NOTIFICATION RESPONSE message. When the establishment of an RR connection is indicated by the RR sublayer (this indication implies that the CM SERVICE REQUEST or NOTIFICATION RESPONSE message has been successfully transferred via the radio interface, see section 2.2), the MM sublayer of the mobile station starts timer T3230, gives an indication to the CM entity that requested the MM connection establishment, and enters MM sublayer state WAIT FOR OUTGOING MM CONNECTION.

b) If an RR connection is available, the MM sublayer of the mobile station sends a CM SERVICE REQUEST or NOTIFICATION RESPONSE message to the network, starts timer T3230, gives an indication to the CM entity that requested the MM connection establishment, and enters:

   - MM sublayer state WAIT FOR OUTGOING MM CONNECTION, if no MM connection is active;

   - MM sublayer state WAIT FOR ADDITIONAL OUTGOING MM CONNECTION, if at least one MM connection is active;

   - If an RR connection exists but the mobile station is in the state WAIT FOR NETWORK COMMAND then any requests from the CM layer that are received will either be rejected or delayed until this state is left.

c) Only applicable for mobile stations supporting VGCS talking:

If a mobile station which is in the MM sublayer state MM IDLE, service state RECEIVING GROUP CALL (NORMAL SERVICE), receives a request from the GCC sublayer to perform an uplink access, the MM sublayer requests the RR sublayer to perform an uplink access procedure and enters MM sublayer state WAIT FOR RR CONNECTION (GROUP TRANSMIT MODE).

When a successful uplink access is indicated by the RR sublayer, the MM sublayer of the mobile station gives an indication to the GCC sublayer and enters MM sublayer state MM CONNECTION ACTIVE (GROUP TRANSMIT MODE).

When an uplink access reject is indicated by the RR sublayer, the MM sublayer of the mobile station gives an indication to the GCC sublayer and enters the MM sublayer state MM IDLE, service state RECEIVING GROUP CALL (NORMAL SERVICE).

In the network, if an uplink access procedure is performed, the RR sublayer in the network provides an indication to the MM sublayer together with the mobile subscriber identity received in the TALKER INDICATION message. The network shall then enter the MM sublayer state MM CONNECTION ACTIVE (GROUP TRANSMIT MODE).

The CM SERVICE REQUEST message contains the

- mobile identity according to section 10.5.1.4;
- mobile station classmark 2;
- ciphering key sequence number; and
- CM service type identifying the requested type of transaction (e.g. mobile originating call establishment, emergency call establishment, short message service, supplementary service activation), location services)

A MS supporting eMLPP may optionally include a priority level in the CM SERVICE REQUEST message.

Only applicable for mobile stations supporting VGCS listening or VBS listening:

The NOTIFICATION RESPONSE message is used if a mobile station has received a notification message on the NCH for a VGCS or VBS call without a description of the respective VGCS or VBS channel. The mobile station therefore establishes an MM connection with a NOTIFICATION RESPONSE in order to obtain the necessary details from the network. The NOTIFICATION RESPONSE message contains the

- mobile identity according to section 10.5.1.4;
- mobile station classmark 2; and
- notified voice group or broadcast call reference according to section 10.5.1.9.

A collision may occur when a CM layer message is received by the mobile station in MM sublayer state WAIT FOR OUTGOING MM CONNECTION or in WAIT FOR ADDITIONAL OUTGOING MM CONNECTION. In this case the MM sublayer in the MS shall establish a new MM connection for the incoming CM message as specified in 4.5.1.3.

Upon receiving a CM SERVICE REQUEST or NOTIFICATION RESPONSE message, the network shall analyse its content. The type of semantic analysis may depend on other on going MM connection(s). Depending on the type of request and the current status of the RR connection, the network may start any of the MM common procedures and RR procedures.

The network may initiate the classmark interrogation procedure, for example, to obtain further information on the mobile station's encryption capabilities.

The identification procedure (see section 4.3.3) may be invoked for instance if a TMSI provided by the mobile station is not recognized.

The network may invoke the authentication procedure (see section 4.3.2) depending on the CM service type.

The network decides also if the ~~ciphering~~security mode setting procedure shall be invoked (see section 3.4.7).

NOTE: If the CM_SERVICE_REQUEST message contains a priority level the network may use this to perform queuing and pre-emption as defined in GSM 03.67.

An indication from the RR sublayer that the ~~ciphering~~security mode setting procedure is completed, or reception of a CM SERVICE ACCEPT message, shall be treated as a service acceptance indication by the mobile station. The MM connection establishment is completed, timer T3230 shall be stopped, the CM entity that requested the MM connection shall be informed, and MM sublayer state MM CONNECTION ACTIVE is entered. The MM connection is considered to be active.

If the service request cannot be accepted, the network returns a CM SERVICE REJECT message to the mobile station.

The reject cause information element (see 10.5.3.6 and Annex G) indicates the reason for rejection. The following cause values may apply:

#4 :	IMSI unknown in VLR
#6 :	Illegal ME
#17 :	Network failure
#22 :	Congestion
#32 :	Service option not supported

#33 : Requested service option not subscribed

#34 : Service option temporarily out of order

If no other MM connection is active, the network may start the RR connection release (see section 3.5) when the CM SERVICE REJECT message is sent.

If a CM SERVICE REJECT message is received by the mobile station, timer T3230 shall be stopped, the requesting CM sublayer entity informed. Then the mobile station shall proceed as follows:

- If the cause value is not #4 or #6 the MM sublayer returns to the previous state (the state where the request was received). Other MM connections shall not be affected by the CM SERVICE REJECT message.

- If cause value #4 is received, the mobile station aborts any MM connection, deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to NOT UPDATED (and stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. If subsequently the RR connection is released or aborted, this will force the mobile station to initiate a normal location updating). Whether the CM request shall be memorized during the location updating procedure, is a choice of implementation.

- If cause value #6 is received, the mobile station aborts any MM connection, deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to ROAMING NOT ALLOWED (and stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. The mobile station shall consider the SIM as invalid until switch-off or the SIM is removed.

4.5.1.3.1 Mobile Terminating CM Activity

When a CM sublayer entity in the network requests the MM sublayer to establish a MM connection, the MM sublayer will request the establishment of an RR connection to the RR sublayer if no RR connection to the desired mobile station exists. The MM sublayer is informed when the paging procedure is finished (see section 3.3.2) and the mobile station shall enter the MM state WAIT FOR NETWORK COMMAND.

(* editor’s note: this does not appear to be stated any where other than in fig 4.1a. Without this statement, there does not seem to be anything to stop the mobile sending a CM SERVICE REQUEST message which might cross (ambiguously) with a ~~CIPHERING~~SECURITY MODE COMMAND message. *)

When an RR connection is established (or if it already exists at the time the request is received), the MM sublayer may initiate any of the MM common procedures (except IMSI detach); it may request the RR sublayer to perform the RR classmark interrogation procedure, and/or the ~~ciphering~~security mode setting procedure.

When all MM and RR procedures are successfully completed which the network considers necessary, the MM sublayer will inform the requesting mobile terminating CM sublayer entity on the success of the MM connection establishment.

If an RR connection already exists and no MM specific procedure is running, the network may also establish a new mobile terminating MM connection by sending a CM message with a new PD/TI combination.

If the establishment of an RR connection is unsuccessful, or if any of the MM common procedures or the ~~ciphering~~security mode setting fail, this is indicated to the CM layer with an appropriate error cause.

If an RR connection used for a MM specific procedure exists to the mobile station, the CM request may be rejected or delayed depending on implementation. When the MM specific procedure has been completed, the network may use the same RR connection for the delayed CM request.

Only applicable in case of VGCS talking:

In the MM CONNECTION ACTIVE (GROUP TRANSMIT MODE) the mobile station is in RR Group transmit mode. There shall be only one MM connection active.

When in MM CONNECTION ACTIVE (GROUP TRANSMIT MODE) state, the MM sublayer in the network shall reject the request for the establishment of another MM connection by any CM layer.

If the RR sublayer in the network indicates a request to perform a transfer of the mobile station from RR connected mode to RR Group transmit mode which will result in a transition from MM CONNECTION ACTIVE state to MM CONNECTION ACTIVE (GROUP TRANSMIT MODE) state in the MM sublayer, the MM sublayer shall not allow the transition if more than one MM connection is active with the mobile station.

4.5.1.3.2 Mobile Originating CM Activity $(CCBS)$

When a CM sublayer entity in the network requests the MM sublayer to establish a MM connection, the MM sublayer will request the establishment of an RR connection to the RR sublayer if no RR connection to the desired mobile station exists. The MM sublayer is informed when the paging procedure is finished (see section 3.3.2) and the mobile station shall enter the MM state WAIT FOR NETWORK COMMAND.
When an RR connection is established (or if it already exists at the time the request is received), the MM sublayer may initiate any of the MM common procedures (except IMSI detach), it may request the RR sublayer to perform the RR classmark interrogation procedure and/or the ~~ciphering~~security mode setting procedure.
The network should use the information contained in *the Mobile Station Classmark Type* 2 IE on the mobile station’s support for “Network Initiated MO CM Connection Request” to determine whether to:

not start this procedure (eg if an RR connection already exists), or,

to continue this procedure, or,

to release the newly established RR connection.

In the case of a “Network Initiated MO CM Connection Request” the network shall use the established RR connection to send a CM SERVICE PROMPT message to the mobile station.
If the mobile station supports ”Network Initiated MO CM Connection Request”, the MM sublayer of the MS gives an indication to the CM entity identified by the CM SERVICE PROMPT message and enters the MM sublayer state PROCESS CM SERVICE PROMPT. In the state PROCESS CM SERVICE PROMPT the MM sublayer waits for either the rejection or confirmation of the recall by the identified CM entity. Any other requests from the CM entities shall either be rejected or delayed until this state is left.

When the identified CM entity informs the MM sublayer, that it has send the first CM message in order to start the CM recall procedure the MM sublayer enters the state MM CONNECTION ACTIVE.

If the identified CM entity indicates that it will not perform the CM recall procedure the MM sublayer starts timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection.

If the CM SERVICE PROMPT message is received by the MS in MM sublayer states WAIT FOR OUTGOING MM CONNECTION or in WAIT FOR ADDITIONAL OUTGOING MM CONNECTION then the mobile station shall send an MM STATUS message with cause ” Message not compatible with protocol state”.
A mobile that does not support “Network Initiated MO CM Connection Request” shall return an MM STATUS message with cause #97 “message type non-existent or not implemented” to the network.
If the mobile station supports “Network Initiated MO CM Connection Request” but the identified CM entity in the mobile station does not provide the associated support, then the mobile station shall send an MM STATUS message with cause “Service option not supported”. In the case of a temporary CM problem (eg lack of transaction identifiers) then the mobile station shall send an MM STATUS message with cause “Service option temporarily out of order”.
If an RR connection already exists and no MM specific procedure is running, the network may use it to send the CM SERVICE PROMPT message.
If the establishment of an RR connection is unsuccessful, or if any of the MM common procedures or the ~~ciphering~~security mode setting fail, this is indicated to the CM layer in the network with an appropriate error cause.
If an RR connection used for a MM specific procedure exists to the mobile station, the “Network Initiated MO CM Connection Request” may be rejected or delayed depending on implementation. When the MM specific procedure has been completed, the network may use the same RR connection for the delayed “Network Initiated MO CM Connection Request”.

4.5.1.6.1 Call re-establishment, initiation by the mobile station

NOTE: The network is unable to initiate call re-establishment.

If at least one request to re-establish an MM connection is received from a CM entity as a response to the indication that the MM connection is interrupted (see 4.5.2.3.) the mobile station initiates the call re-establishment procedure. If several CM entities request re-establishment only one re-establishment procedure is initiated. If any CM entity requests re-establishment, then re-establishment of all transactions belonging to all Protocol Discriminators that permit Call Re-establishment shall be attempted.

Upon request of a CM entity to re-establish an MM connection the MM sublayer requests the RR sublayer to establish an RR connection and enters MM sublayer state WAIT FOR REESTABLISH. This request contains an establishment cause and a CM RE-ESTABLISHMENT REQUEST message. When the establishment of an RR connection is indicated by the RR sublayer (this indication implies that the CM RE-ESTABLISHMENT REQUEST message has been successfully transferred via the radio interface, see section 2.2), the MM sublayer of the mobile station starts timer T3230, gives an indication to all CM entities that are being re-established, and remains in the MM sublayer state WAIT FOR REESTABLISH.

The CM RE-ESTABLISHMENT REQUEST message contains the

- mobile identity according to section 10.5.1.4;
- mobile station classmark 2;
- ciphering key sequence number.

NOTE: Whether or not a CM entity can request re-establishment depends upon the Protocol Discriminator. The specifications for Short Message Service (GSM 04.11), Call Independent Supplementary Services (TS 24.010) and Location Services (TS 24.071) do not currently specify any re-establishment procedures.

Upon receiving a CM RE-ESTABLISHMENT REQUEST message, the network shall analyse its content. Depending on the type of request, the network may start any of the MM common procedures and RR procedures.

The network may initiate the classmark interrogation procedure, for example, to obtain further information on the mobile station's encryption capabilities.

The identification procedure (see section 4.3.3) may be invoked.

The network may invoke the authentication procedure (see section 4.3.2).

The network decides if the ~~ciphering~~security mode setting procedure shall be invoked (see section 3.4.7).

An indication from the RR sublayer that the ~~ciphering~~security mode setting procedure is completed, or reception of a CM SERVICE ACCEPT message, shall be treated as a service acceptance indication by the mobile station. The MM connection re-establishment is completed, timer T3230 shall be stopped, all CM entities associated with the re-establishment shall be informed, and MM sublayer state MM CONNECTION ACTIVE is re-entered. All the MM connections are considered to be active.

If the network cannot associate the re-establishment request with any existing call for that mobile station, a CM SERVICE REJECT message is returned with the reject cause:

#38	"call cannot be identified"

If call re-establishment cannot be performed for other reasons, a CM SERVICE REJECT is returned, the appropriate reject cause may be any of the following (see annex G):

# 4	"IMSI unknown in VLR";
# 6	"illegal ME";
#17	"network failure";
#22	"congestion";
#32	"service option not supported";
#34	"service option temporarily out of order".

Whatever the reject cause a mobile station receiving a CM SERVICE REJECT as a response to the CM RE-ESTABLISHMENT REQUEST shall stop T3230, release all MM connections and proceed as described in section 4.5.3.1. In addition:

- if cause value #4 is received, the mobile station deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to NOT UPDATED (and stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. If subsequently the RR connection is released or aborted, this will force the mobile station to initiate a normal location updating). The CM re-establishment request shall not be memorized during the location updating procedure.

- if cause value #6 is received, the mobile station deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to ROAMING NOT ALLOWED (and stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. The MS shall consider the SIM as invalid until switch-off or the SIM is removed.

9.2.2 Authentication request

This message is sent by the network to the mobile station to initiate authentication of the mobile station identity. See table 9.2.3/TS 24.008.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to mobile station

Table 9.2.3/TS 24.008: AUTHENTICATION REQUEST message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication Request Message type	Message type 10.4	M	V	1
	Ciphering key sequence Number	Ciphering key sequence Number 10.5.1.2	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
	Authentication Parameter RAND (UMTS challenge or GSM challenge)	Auth. parameter RAND 10.5.3.1	M	V	16
20	Authentication Parameter AUTN	Auth. parameter AUTN 10.5.3.1.2	O	TLV	14-19

9.2.2.1 Authentication Parameter AUTN

This IE shall be present if and only if the authentication challenge is a UMTS authentication challenge. The presence or absence of this IE defines- in the case of its absence- a GSM authentication challenge or- in the case of its presence- a UMTS authentication challenge.

9.2.3 Authentication response

This message is sent by the mobile station to the network to deliver a calculated response to the network. See table 9.2.4/TS 24.008.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: mobile station to network

Table 9.2.4/TS 24.008: AUTHENTICATION RESPONSE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator	M	V	1/2

		10.3.1			
	Authentication Response Message type	Message type 10.4	M	V	1
	Authentication Response Parameter ~~SRES~~	Auth. Response parameter ~~SRES~~ 10.5.3.2	M	V	4
21	Authenticatio Response Parameter (extension)	Auth. Response parameter 10.5.3.2.1	O	TLV	14

9.2.3.1 Authentication Response Parameter

This IE contains the SRES, if it was a GSM authentication challenge, or the RES (all or just the 4 most significant octets of) if it was a UMTS authentication challenge (see also 9.2.3.2).

9.2.3.2 Authentication Response Parameter (extension)

This IE shall be included if and only if the authentication challenge was a UMTS authentication challenge and the RES parameter is greater than 4 octets in length. It shall contain the least significant remaining bits of the RES (the four most significant octets shall be sent in the Authentication Response Parameter IE (see 9.2.3.1))

9.2.3a CS Authentication Failure (UMTS authentication challenge)

This message is sent by the mobile station to the network to indicate that authentication of the network has failed. See table 9.2.4/TS 24.008.

Message type:CS AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.2.4/TS 24.008: CS AUTHENTICATION FAILURE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	CS Authentication Failure Message type	Message type 10.4	M	V	1
	Reject Cause	Reject Cause 10.5.3.6	M	V	1
22	Response from SIM	Response from SIM 10.5.3.2.2	O	TLV	30 - 32

9.2.3a.1 Response from SIM

This IE shall be sent if and only if the reject cause was ‘CS synch failure.’ It shall include the response to the authentication challenge from the SIM, which is made up of the RAND$_{MS}$ and the AUTS parameters (see TS 33.102).

9.2.4 CM Re-establishment request

This message is sent by the mobile station to the network to request re-establishment of a connection if the previous one has failed. See table 9.2.5/TS 24.008.

Message type:CM RE-ESTABLISHMENT REQUEST

Significance: dual

Direction: mobile station to network

Table 9.2.5/TS 24.008: CM RE-ESTABLISHMENT REQUEST message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	~~1/2~~½
	Skip Indicator	Skip Indicator 10.3.1	M	V	~~1/2~~½
	CM Re-Establishment Request message type	Message type 10.4	M	V	1
	Ciphering key sequence Number	Ciphering key sequence Number 10.5.1.2	M	V	~~1/2~~½
	Spare half octet	Spare half octet 10.5.1.8	M	V	~~1/2~~½
	Mobile station Classmark	Mobile station Classmark 2 10.5.1.6	M	LV	4
	Mobile identity	Mobile identity 10.5.1.4	M	LV	2-9
13	Location area Identification	Location area Identification 10.5.1.3	C	TV	6

9.2.4.1 Location area identification

The *location area identification* information element shall appear when a TMSI is used as mobile identity, to render that mobile identity non-ambiguous. This is the LAI stored in the SIM.

9.2.4.2 Mobile Station Classmark

This IE shall include for multiband mobile station the Classmark 2 corresponding to the frequency band in use.

9.2.9 CM service request

This message is sent by the mobile station to the network to request a service for the connection management sublayer entities, e.g. circuit switched connection establishment, supplementary services activation, short message transfer, location services. See table 9.2.11/TS 24.008.

Message type:CM SERVICE REQUEST

Significance: dual

Direction: mobile station to network

Table 9.2.11/TS 24.008: CM SERVICE REQUEST message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Skip Indicator	Skip Indicator 10.3.1	M	V	~~1/2~~½
	CM Service Request Message type	Message type 10.4	M	V	1
	CM service type	CM service type 10.5.3.3	M	V	~~1/2~~½
	Ciphering key sequence Number	Ciphering key sequence Number	M	V	~~1/2~~½

		10.5.1.2			
	Mobile station Classmark	Mobile station Classmark 2 10.5.1.6	M	LV	4
	Mobile identity	Mobile identity 10.5.1.4	M	LV	2-9
8-	Priority	Priority Level 10.5.1.11	O	TV	1

9.2.9.1 Mobile Station Classmark

This IE shall include for multiband mobile station the Classmark 2 corresponding to the frequency band in use.

9.2.9.2 Priority

May be included by mobile station supporting eMLPP to indicate the priority requested.
This information element is only meaningful when the CM service type is:

Mobile originating call establishment;

Emergency call establishment;

Voice group call establishment;

Voice broadcast call establishment.

9.2.15 Location updating request

This message is sent by the mobile station to the network either to request update of its location file (normal updating or periodic updating) or to request IMSI attach. See table 9.2.17/TS 24.008.

Message type:LOCATION UPDATING REQUEST

Significance: dual

Direction: mobile station to network

Table 9.2.17/TS 24.008: LOCATION UPDATING REQUEST message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Location Updating Request message type	Message type 10.4	M	V	1
	Location updating type	Location updating type 10.5.3.5	M	V	1/2
	Ciphering key sequence Number	Ciphering key sequence Number 10.5.1.2	M	V	1/2
	Location area Identification	Location area Identification 10.5.1.3	M	V	5
	Mobile station Classmark	Mobile station Classmark 1 10.5.1.5	M	V	1
	Mobile identity	Mobile identity 10.5.1.4	M	LV	2-9

9.2.15.1 Location area identification

The location area identification stored in the SIM is used.

9.2.15.2 Mobile Station Classmark

This IE shall include for multiband MS the Classmark 1 corresponding to the frequency band in use.

GMM

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:

- to permit the network to check whether the identity provided by the MS is acceptable or not, see GSM 03.20 [13]);
- to provide parameters enabling the MS to calculate a new GPRS ciphering key sequence number.
- to let the network set the security mode (security/no security) and algorithm; and
- To permit the receiving entity to check the integrity of signalling messages.

In UMTS, 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 GSM 02.09 [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.
A R99 GPRS-only MS connected to a R99 core network (even using the BSS radio access) shall support a UMTS authentication challenge.

In the case of a UMTS authentication challenge in a GSM system the authentication and ciphering procedure can be used for either:

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

4.7.7b Authentication and ciphering procedure used for GSM authentication challenge

The purpose of the authentication and ciphering procedure is threefold:

- to permit the network to check whether the identity provided by the MS is acceptable or not, see GSM 03.20 [13]);
- to provide parameters enabling the MS to calculate a new GPRS ciphering key; and
- In GSM, to let the network set the ciphering mode (ciphering/no ciphering) and algorithm.

In GSM, ~~T~~the authentication and ciphering procedure can be used for either:

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

The cases in which the authentication and ciphering procedure shall be used are defined in GSM 02.09 [5].

In GSM, ~~T~~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 ciphering key should be used instead of the old one.

The network should not send any user data during the authentication and ciphering procedure.

4.7.7.1 Authentication and ciphering initiation by the network

The network initiates the authentication and ciphering procedure by transferring an AUTHENTICATION AND CIPHERING REQUEST message across the radio interface and starts timer T3360. The AUTHENTICATION AND CIPHERING REQUEST message shall contain all parameters necessary to calculate the response parameters when authentication is performed (see GSM 03.20 [13]).
If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain either:

- In a GSM authentication challenge, the GPRS ciphering key sequence number, allocated to the GPRS ciphering key and the RAND;or

- In a UMTS authentication challenge, the GPRS ciphering key sequence number, allocated to the ciphering and integrity keys, the RAND and the AUTN.

In GSM, ~~I~~if authentication is not requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall not contain neither the GPRS ciphering key sequence number nor the RAND.
In GSM, ~~I~~if ciphering is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall indicate the GPRS ciphering algorithm.

The network includes the A&C reference number information element in the AUTHENTICATION AND CIPHERING REQUEST message. Its value is chosen in order to link an AUTHENTICATION AND CIPHERING REQUEST in a RA with its RESPONSE. The A&C reference number value might be based on the RA Colour Code value.
Additionally, the network may request the MS to include its IMEISV in the AUTHENTICATION AND CIPHERING RESPONSE message.

4.7.7.2 Authentication and ciphering response by the MS

An MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time.

In a GSM authentication challenge, ~~I~~if the AUTHENTICATION AND CIPHERING REQUEST message includes the authentication parameters RAND and GPRS CKSN, then upon receipt of the message, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message.The new GPRS ciphering key calculated from the challenge information shall overwrite the previous one. It shall be stored and shall be loaded into the ME before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The GPRS ciphering key sequence number shall be stored together with the calculated ciphering key.

In a UMTS authentication challenge, ~~I~~if the AUTHENTICATION AND CIPHERING REQUEST message includes the UMTS authentication parameters GPRS CKSN, RAND and AUTN, then upon receipt of the message, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message. The new ciphering keys calculated from the challenge information shall overwrite the previous ones and be stored on the SIM before the AUTHENTICATION RESPONSE message is transmitted. The ciphering keys stored on the SIM shall be loaded into the ME when any valid

SECURITY MODE COMMAND is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in GSM04.18 section 3.4.7.2).,

In GSM, ~~I~~if the AUTHENTICATION AND CIPHERING REQUEST message does not include either the GPRS or the UMTS authentication parameters (RAND and GPRS CKSNor RAND, AUTN and GPRS CKSN), then upon receipt of the message, the MS replies by sending an AUTHENTICATION AND CIPHERING RESPONSE message to the network.

In GSM, ~~T~~the GMM layer shall notify the LLC layer if ciphering shall be used or not and if yes which algorithm and GPRS ciphering key that shall be used (see GSM 04.64 [76]).

4.7.7.3 Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see GSM 03.20 [13]). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent.
In GSM, ~~T~~the GMM layer shall notify the LLC sublayer if ciphering shall be used or not and if yes which algorithm and GPRS ciphering key that shall be used (see GSM 04.64 [76]).

4.7.7.4 GPRS ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets, i.e. from a challenge parameter RAND both the authentication response parameter~~SRES~~ and the GPRS ciphering key can be computed given the secret key associated to the IMSI.
In order to allow start of ciphering on a logical link without authentication, GPRS ciphering key sequence numbers are introduced.
The sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the sequence number allocated to the key(s) which may be computed from the RAND parameter carried in that message.
The MS stores this number with the key(s), and includes the corresponding sequence number in the ROUTING AREA UPDATE REQUEST and ATTACH REQUEST messages. If the sequence number is deleted, the associated key(s) shall be considered as invalid.
The network may choose to start ciphering with the stored key (under the restrictions given in GSM 02.09) if the stored sequence number and the one given from the MS are equal and the previously negotiated ciphering algorithm is known and supported in the network. When ciphering is requested at GPRS attach, the authentication and ciphering procedure shall be performed since the MS does not store the ciphering algorithm at detach.
Upon GPRS attach, if ciphering is to be used, an AUTHENTICATION AND CIPHERING REQUEST message shall be sent to the MS to start ciphering.
If the GPRS ciphering key sequence number stored in the network does not match the GPRS ciphering key sequence number received from the MS in the ATTACH REQUEST message, then the network should authenticate the MS.

In GSM, ~~T~~the MS starts ciphering after sending the AUTHENTICATION AND CIPHERING RESPONSE message. The SGSN starts ciphering when a valid AUTHENTICATION AND CIPHERING RESPONSE is received from the MS.

In UMTS, see specification TS 25.331

In GSM, ~~A~~as an option, the network may decide to continue ciphering without sending an AUTHENTICATION AND CIPHERING REQUEST message after receiving a ROUTING AREA UPDATE REQUEST message with a valid GPRS ciphering key sequence number. Both the MS and the network shall use the latest ciphering parameters. The SGSN starts ciphering when sending the ciphered ROUTING AREA UPDATE ACCEPT message to the MS. The MS starts ciphering after receiving a valid ciphered ROUTING AREA UPDATE ACCEPT message from the network.

In UMTS, ciphering for the PS domain is described in TS 25.331.

4.7.7.5 ~~Unsuccessful a~~Authentication not accepted by the network ~~and ciphering~~

If authentication and ciphering fails, i.e. if the response is not valid, the network considers whether the MS has used the P-TMSI or the IMSI for identification.

- If the P-TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the MS differs from the one the network had associated with the P-TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

- If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION AND CIPHERING REJECT message should be transferred to the MS.

Upon receipt of an AUTHENTICATION AND CIPHERING REJECT message, the MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. If available, also the TMSI~~,~~ LAI~~,~~ and ciphering key sequence number shall be deleted and the update status shall be set to U3 ROAMING NOT ALLOWED. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

4.7.7.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.
Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see TS 33.102). This parameter contains two possible causes for authentication failure:

a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a PS AUTHENTICATION FAILURE message (9.2.3a) to the network, with the failure cause 'PS MAC failure' and parameters provided by the SIM (see TS 33.102). Thereafter the procedural behaviour is ffs.

b) SQN failure

If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a PS AUTHENTICATION FAILURE message (9.2.3a) to the network, with the failure cause 'PS Synch failure' and parameters provided by the SIM (see 33.102) Upon receipt of this message, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

Note: Actions might vary according to the presence/absence of an integrity protected connection to a different core network node.

4.7.7.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

Upon detection of a lower layer failure before the AUTHENTICATION AND CIPHERING RESPONSE is received, the network shall abort the procedure.

b) Expiry of timer T3360

The network shall, on the first expiry of the timer T3360, retransmit the AUTHENTICATION AND CIPHERING REQUEST and shall reset and start timer T3360. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3360, the procedure shall be aborted.

c) Collision of an authentication and ciphering procedure with a GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and no GPRS attach procedure is pending on the network (i.e. no ATTACH ACCEPT/REJECT message has to be sent as an answer to an ATTACH REQUEST message), the network shall abort the authentication and ciphering procedure and proceed with the new GPRS attach procedure.

d) Collision of an authentication and ciphering procedure with a GPRS attach procedure when the authentication and ciphering procedure has been caused by a previous GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and a GPRS attach procedure is pending (i.e. an ATTACH ACCEPT/REJECT message has still to be sent as an answer to an earlier ATTACH REQUEST message), then:

- If one or more of the information elements in the ATTACH REQUEST message differs from the ones received within the previous ATTACH REQUEST message, the network shall not treat the authentication any further and proceed with the GPRS attach procedure ; or

- If the information elements do not differ, then the network shall not treat any further this new ATTACH REQUEST.

Collision of an authentication and ciphering procedure with a GPRS detach procedure

GPRS detach containing cause "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall abort the authentication and ciphering procedure and shall progress the GPRS detach procedure.

GPRS detach containing other causes than "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall complete the authentication and ciphering procedure and shall respond to the GPRS detach procedure as described in section 4.7.4.

e) Collision of an authentication and ciphering procedure with a routing area updating procedure

If the network receives a ROUTING AREA UPDATE REQUEST message before the ongoing authentication procedure has been completed, the network shall progress both procedures.

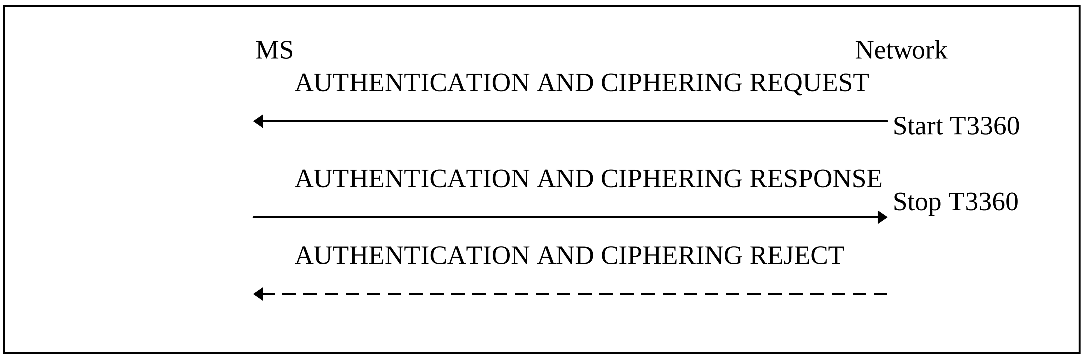
MS
Network
AUTHENTICATION AND CIPHERING REQUEST
Start T3360
AUTHENTICATION AND CIPHERING RESPONSE
Stop T3360
AUTHENTICATION AND CIPHERING REJECT

Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

9.4.9 Authentication and ciphering request

This message is sent by the network to the MS to initiate authentication of the MS identity. Additionally, the ciphering mode is set, indicating whether ciphering will be performed or not. See table 9.4.9/TS 24.008.

Message type: AUTHENTICATION AND CIPHERING REQUEST

Significance: dual

Direction: network to MS

Table 9.4.9/TS 24.008: AUTHENTICATION AND CIPHERING REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Authentication and ciphering request message identity	Message type 10.4	M	V	1
	Ciphering algorithm	Ciphering algorithm 10.5.5.3	M	V	1/2
	IMEISV request	IMEISV request 10.5.5.10	M	V	1/2
	Force to standby	Force to standby 10.5.5.7	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
	A&C reference number	A&C reference number 10.5.5.19	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
21	Authentication parameter RAND	Authentication parameter RAND 10.5.3.1	O	TV	17
8	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	C	TV	1
28	Authentication parameter AUTN	Authentication parameter AUTN 10.5.3.1.2	O	TLV	14-19

9.4.9.1 Authentication Parameter RAND

This IE shall only be included if authentication shall be performed.

9.4.9.2 GPRS ciphering key sequence number

This IE is included if and only if the *Authentication parameter RAND* is contained in the message.

9.4.9.3 Authentication Parameter AUTN

This IE shall be present if and only if the authentication challenge is a UMTS authentication challenge.The presence or absence of this IE defines- in the case of its absence- a GSM authentication challenge or- in the case of its presence- a UMTS authentication challenge.

9.4.10 Authentication and ciphering response

This message is sent by the MS to the network in response to an *Authentication and ciphering request* message. See table 9.4.10/TS 24.008.

Message type:AUTHENTICATION AND CIPHERING RESPONSE

Significance: dual

Direction: MS to network

Table 9.4.10/TS 24.008: AUTHENTICATION AND CIPHERING RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Authentication and ciphering response message identity	GPRS message type 10.4	M	V	1
	A&C reference number	A&C reference number 10.5.5.19	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
23	IMEISV	Mobile identity 10.5.1.4	O	TLV	11
22	Authentication Response parameter ~~SRES~~	Authentication Response parameter ~~SRES~~ 10.5.3.2	O	TV	5
29	Authentication Response parameter (extension)	Authentication Response parameter 10.5.3.2.1	O	TLV	14

9.4.10.1 IMEISV

This IE is included if requested within the corresponding *authentication and ciphering request* message.

9.4.10.2 Authentication Response Parameter ~~SRES~~

This IE is included if authentication was requested within the corresponding *authentication and ciphering request* message. This IE contains the SRES, if the authentication challenge was for GSM or the RES (all or just the 4 most significant octets of) if it is a UMTS authentication challenge (see also 9.4.10.2).

9.4.10.3 Authentication Response Parameter (extension)

This IE shall be included if and only if the authentication challenge was a UMTS authentication challenge and the RES parameter is greater than 4 octets in length. It shall contain the least significant remaining bits of the RES (the four most significant octets shall be sent in the Authentication Response Parameter IE (see 9.2.3.1))

9.4.10a PS Authentication Failure (UMTS authentication challenge)

This message is sent by the mobile station to the network to indicate that authentication of the network has failed. See table 9.4.10a/TS 24.008.

Message type: PS AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.4.10a/TS 24.008: PS AUTHENTICATION FAILURE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	PS Authentication Failure Message type	Message type 10.4	M	V	1

	GMM Cause	GMM Cause 10.5.5.14	M	V	1
30	Response from SIM	Response from SIM 10.5.3.2.2	O	T	30 - 32

9.4.10a.1 Response from SIM

This IE shall be sent if and only if the GMM cause was ‘PS synch failure.’ It shall include the response to the authentication challenge from the SIM, which is made up of the RAND_{MS} and the AUTS parameters (see TS 33.102).

9.4.14 Routing area update request

This message is sent by the MS to the network either to request an update of its location file or to request an IMSI attach for non-GPRS services. See table 9.4.14/TS 24.008.

Message type:ROUTING AREA UPDATE REQUEST

Significance: dual

Direction: MS to network

Table 9.4.14/TS 24.008: ROUTING AREA UPDATE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Routing area update request message identity	Message type 10.4	M	V	1
	Update type	Update type 10.5.5.18	M	V	1/2
	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	1/2
	Old routing area identification	Routing area identification 10.5.5.15	M	V	6
	MS Radio Access capability	MS Radio Access capability 10.5.5.12a	M	LV	6 - 14
19	Old P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
17	Requested READY timer value	GPRS Timer 10.5.7.3	O	TV	2
27	DRX parameter	DRX parameter 10.5.5.6	O	TV	3

9.4.14.1 Old P-TMSI signature

This IE is included by the MS if it was received from the network in an ATTACH ACCEPT or ROUTING AREA UPDATE ACCEPT message.

9.4.14.2 Requested READY timer value

This IE may be included if the MS wants to indicate a preferred value for the READY timer.

9.4.14.3 DRX parameter

This IE may be included if the MS wants to indicate new DRX parameters.

10.4 Message Type

The message type IE and its use are defined in TS 24.007 [20]. Tables 10.3/TS 24.008, 10.4/TS 24.008, and 10.4a/TS 24.008 define the value part of the message type IE used in the Mobility Management protocol, the Call Control protocol, and Session management protocol.

Table 10.2/TS 24.008: Message types for Mobility Management

8	7	6	5	4	3	2	1	
0	x	0	0	-	-	-	-	Registration messages:
				0	0	0	1	- IMSI DETACH INDICATION
				0	0	1	0	- LOCATION UPDATING ACCEPT
				0	1	0	0	- LOCATION UPDATING REJECT
				1	0	0	0	- LOCATION UPDATING REQUEST
0	x	0	1	-	-	-	-	Security messages:
				0	0	0	1	- AUTHENTICATION REJECT
				0	0	1	0	- AUTHENTICATION REQUEST
				0	1	0	0	- AUTHENTICATION RESPONSE
				1	1	0	0	- CS AUTHENTICATION FAILURE
				1	0	0	0	- IDENTITY REQUEST
				1	0	0	1	- IDENTITY RESPONSE
				1	0	1	0	- TMSI REALLOCATION COMMAND
				1	0	1	1	- TMSI REALLOCATION COMPLETE
0	x	1	0	-	-	-	-	Connection management messages:
				0	0	0	1	- CM SERVICE ACCEPT
				0	0	1	0	- CM SERVICE REJECT
				0	0	1	1	- CM SERVICE ABORT
				0	1	0	0	- CM SERVICE REQUEST
				0	1	0	1	- CM SERVICE PROMPT
				0	1	1	0	- NOTIFICATION RESPONSE
				1	0	0	0	- CM RE-ESTABLISHMENT REQUEST
				1	0	0	1	- ABORT
0	x	1	1	-	-	-	-	Miscellaneous messages:
				0	0	0	0	- MM NULL
				0	0	0	1	- MM STATUS
				0	0	1	0	- MM INFORMATION

Bit 8 is reserved for possible future use as an extension bit, see TS 24.007.
Bit 7 is reserved for the send sequence number in messages sent from the mobile station. In messages sent from the network, bit 7 is coded with a "0". See TS 24.007.

Table 10.4/TS 24.008: Message types for GPRS mobility management

Bits 8	 7	 6	 5	 4	 3	 2	 1	
0	0	-	-	-	-	-	-	Mobility management messages
0	0	0	0	0	0	0	1	Attach request
0	0	0	0	0	0	1	0	Attach accept
0	0	0	0	0	0	1	1	Attach complete
0	0	0	0	0	1	0	0	Attach reject
0	0	0	0	0	1	0	1	Detach request
0	0	0	0	0	1	1	0	Detach accept
0	0	0	0	1	0	0	0	Routing area update request
0	0	0	0	1	0	0	1	Routing area update accept
0	0	0	0	1	0	1	0	Routing area update complete
0	0	0	0	1	0	1	1	Routing area update reject
0	0	0	1	0	0	0	0	P-TMSI reallocation command
0	0	0	1	0	0	0	1	P-TMSI reallocation complete
0	0	0	1	0	0	1	0	Authentication and ciphering req
0	0	0	1	0	0	1	1	Authentication and ciphering resp
0	0	0	1	0	1	0	0	Authentication and ciphering rej
0	0	0	1	1	1	0	0	PS Authentication Failure
0	0	0	1	0	1	0	1	Identity request
0	0	0	1	0	1	1	0	Identity response
0	0	1	0	0	0	0	0	GMM status
0	0	1	0	0	0	0	1	GMM information

10.5.1.2 Ciphering Key Sequence Number

In a GSM authentication challenge, ~~T~~the purpose of the *Ciphering Key Sequence Number* information element is to make it possible for the network to identify the ciphering key Kc which is stored in the mobile station without invoking the authentication procedure.

The ciphering key sequence number is allocated by the network and sent with the AUTHENTICATION REQUEST message to the mobile station where it is stored together with the calculated ciphering key Kc. The *Ciphering Key Sequence Number* information element is coded as shown in figure 10.5.2/TS 24.008 and table 10.5.2/TS 24.008.

In a UMTS authentication challenge, the purpose of the *Ciphering Key Sequence Number* information element is to make it possible for the network to identify the ciphering key CK and integrity key IK which are stored in the MS without invoking the authentication procedure. CK and IK form a Key Set Identifier (KSI) (see TS 33.102) which is encoded the same as the CKSN and is therefore included in the CKSN field.

The ciphering key sequence number is a type 1 information element.

```
    8     7     6     5     4     3     2     1
 +-----------------------------------------------+
 |     |Ciphering Key    _|     |   key sequence   |  octet 1
 |     |Sequence Number  _|  0  |                  |
 |     |      IEI        _|spare|                  |
 +-----------------------------------------------+
```

Figure 10.5.2/TS 24.008 *Ciphering Key Sequence Number* information element

Table 10.5.2/TS 24.008: *Ciphering Key Sequence Number* information element

```
+---------------------------------------------------+
| Key sequence (octet 1)                            |
|                                                   |
| Bits                                              |
| 3 2 1                                             |
|                                                   |
| 0 0 0                                             |
| through  Possible values for the ciphering key    |
| 1 1 0     sequence number                         |
|                                                   |
| 1 1 1    No key is available (MS to network);    |
|          Reserved (network to MS)                 |
+---------------------------------------------------+
```

10.5.3 Mobility management information elements.

10.5.3.1 Authentication parameter RAND

The purpose of the *Authentication Parameter RAND* information element is to provide the mobile station with a non-predictable number to be used to calculate the authentication response signature SRES and the ciphering key Kc (for a GSM authentication challenge), or the response RES and both the ciphering key CK and integrity key IK (for a UMTS authentication challenge).

The *Authentication Parameter RAND* information element is coded as shown in figure 10.5.75/TS 24.008 and table 10.5.89/TS 24.008.

The *Authentication Parameter RAND* is a type 3 information element with 17 octets length.

```
    8     7     6     5     4     3     2     1
 +-----------------------------------------------+
 |        Authentication parameter RAND IEI      |  octet 1
 +-----------------------------------------------+
 |                                               |
 |                  RAND value                   |  octet 2
                       :
                       :
 |                                               |  octet 17
 |                                               |
 +-----------------------------------------------+
```

Figure 10.5.75/TS 24.008 *Authentication Parameter RAND* information element

Table 10.5.89/TS 24.008: *Authentication Parameter RAND* information element

```
 +-------------------------------------------------------+
 | RAND value (octet 2, 3,... and 17)                    |
 | The RAND value consists of 128 bits. Bit 8 of octet   |
 | 2  is the most significant bit while bit 1 of octet   |
 | 17 is the least significant bit.                      |
 +-------------------------------------------------------+
```

10.5.3.1.2 Authentication Parameter AUTN (UMTS authentication challenge only)

The purpose of the *Authentication Parameter AUTN* information element is to provide the MS with a means of authenticating the network.

The *Authentication Parameter AUTN* information element is coded as shown in figure 10.5.75.1/TS 24.008 and table 10.5.89.1/TS 24.008.

The *Authentication Parameter AUTN* is a type 4 information element with a minimum of 14 octets and a maximum of 19 octets length.

Figure 10.5.75.1/TS 24.008 *Authentication Parameter AUTN* information element (UMTS authentication challenge only)

8 7 6 5 4 3 2 1	
Authentication Parameter AUTN IEI	octet 1
Length of AUTN contents	octet 2
AUTN	Octet 3 octet 19

Table 10.5.89.1/TS 24.008 *Authentication Parameter AUTN* information element (UMTS authentication challenge only)

```
+-------------------------------------------------------+
| AUTN value (octets 3 to 19)                           |
|                                                       |
| The AUTN consists of (SQN xor AK)||MODE||MAC          |
|                     =(32 to 64)+1+64 bits             |
|                      (see TS 33.102)                  |
|                                                       |
+-------------------------------------------------------+
```

10.5.3.2 Authentication Response parameter ~~SRES~~

The purpose of the *authentication response parameter* ~~*SRES*~~ information element is to provide the network with the authentication response ~~signature~~ calculated in the ~~mobile station~~SIM.
The *Authentication Response Parameter* ~~*SRES*~~ information element is coded as shown in figure 10.5.76/TS 24.008 and tables 10.5.90a & b/TS 24.008.
The *Authentication Response Parameter* ~~*SRES*~~ is a type 3 information element with 5 octets length.

In a GSM authentication challenge, the response calculated in the SIM (SRES) is 4 bytes in length, and is placed in the *Authentication Response Parameter* information element.

In a UMTS authentication challenge, ~~T~~the response calculated in the SIM (RES) may be up to 16 octets in length. The 4 most significant octets shall be included in the *Authentication Response Parameter* information element. The remaining part of the RES shall be included in the Authentication Response Parameter (extension) IE (see 10.5.3.2.1)

```
    8     7     6     5     4     3     2     1
+-----------------------------------------------+
|      Authentication Response parameter ~~SRES~~ IEI  | octet 1
+-----------------------------------------------+
|                                               |
|        SRES value or most significant         | octet 2
|                   4 octets of RES             |
                        :
                        :
|                                               | octet 5
|                                               |
+-----------------------------------------------+
```

Figure 10.5.76/TS 24.008 *Authentication Response Parameter ~~SRES~~* information element

Table 10.5.90a/TS 24.008: *Authentication Response Parameter ~~SRES~~* information element (SRES) (GSM only)

```
+-------------------------------------------------------+
| SRES value (octet 2, 3, 4 and 5)                      |
| The SRES value consists of 32 bits. Bit 8 of octet 2  |
| is  the  most significant bit while bit 1 of octet 5  |
| is the least significant bit.                         |
+-------------------------------------------------------+
```

Table 10.5.90b/TS 24.008: *Authentication Response Parameter* information element (RES) (UMTS only)

```
+-------------------------------------------------------+
| RES value (octet 2, 3, 4 and 5)                      |
|                                                       |
| This contains the  most significant 4 octets of RES   |
| If RES>4 octets, the remaining octets of RES shall   |
| appear in the Authentication Response Parameter       |
| (extension) IE (see 10.5.3.2.1)                       |
+-------------------------------------------------------+
```

10.5.3.2.1 Authentication Response Parameter (extension) (UMTS authentication challenge only)

This IE is included if the authentication response parameter RES is longer than 4 octets (UMTS only) and therefore does not fit in the Authentication Response Parameter field (see 10.5.3.2).
The Authentication Response parameter (extension) IE is coded as shown in figure 10.5.76.1/TS 24.008 and table 10.5.90.1/TS 24.008.
The Authentication Response parameter (extension) IE is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets.

Figure 10.5.76.1/TS 24.008 Authentication Response Parameter (extension) information element (UMTS only)

8 7 6 5 4 3 2 1	
Authentication Response (extension) IEI	octet 1
Length of Authentication Response contents	octet 2
RES (all but 4 most significant octets)	octet 3
:	
:	
	octet 14

Table 10.5.90.1/TS 24.008: *Authentication Response Parameter (extension)* information element (RES)

```
+-----------------------------------------------------+
| RES (extension) value (octet 3 to 14)                |
|                                                      |
| This contains all but the 4 most significant octets  |
|  of RES                                              |
|                                                      |
+-----------------------------------------------------+
```

10.5.3.2.2 Response from SIM (UMTS authentication challenge only)

The purpose of the *Response from SIM* information element is to provide the network with the necessary information to begin a re-authentication procedure (see TS 33.102) in the case of a 'PS synch failure' or a 'CS synch failure,' following a UMTS authentication challenge.
The Response from SIM IE is coded as shown in figure 10.5.76.2/TS 24.008 and table 10.5.90.2/TS 24.008.
The Response from SIM IE is a type 4 information element with a minimum length of 30 octets and a maximum length of 32 octets.

Figure 10.5.76.2/TS 24.008 *Response from SIM* information element (UMTS authentication challenge only)

8	7	6	5	4	3	2	1	
Response from SIM IEI								octet 1
Length of Response from SIM contents								octet 2
Response from SIM : :								octet 3 octet 32

Table 10.5.90.2/TS 24.008: *Response from SIM* information element

Response from SIM value (octet 3 to 32)
This contains $RAND_{MS}$ and AUTS (see TS 33.102)

10.5.3.6 Reject cause

The purpose of the *Reject Cause* information element is to indicate the reason why a request from the mobile station is rejected by the network.

The *Reject Cause* information element is coded as shown in figure 10.5.81/TS 24.008 and table 10.5.95/TS 24.008.

The *Reject Cause* is a type 3 information element with 2 octets length.

8	7	6	5	4	3	2	1	
Reject cause IEI								octet 1
reject cause value								octet 2

Figure 10.5.81/TS 24.008 *Reject Cause* information element

Table 10.5.95/TS 24.008: *Reject Cause* information element

Reject cause value (octet 2)

Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	0	IMSI unknown in HLR
0	0	0	0	0	0	1	1	Illegal MS
0	0	0	0	0	1	0	0	IMSI unknown in VLR
0	0	0	0	0	1	0	1	IMEI not accepted
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	1	0	1	1	PLMN not allowed
0	0	0	0	1	1	0	0	Location Area not allowed
0	0	0	0	1	1	0	1	Roaming not allowed in this location area
0	0	0	0	0	1	1	1	CS MAC failure
0	0	0	0	1	1	1	1	CS Synch failure
0	0	0	1	0	0	0	1	Network failure
0	0	0	1	0	1	1	0	Congestion
0	0	1	0	0	0	0	0	Service option not supported
0	0	1	0	0	0	0	1	Requested service option not subscribed
0	0	1	0	0	0	1	0	Service option temporarily out of order
0	0	1	0	0	1	1	0	Call cannot be identified
0	0	1	1	0	0	0	0	}
			to					} retry upon entry into a new cell
0	0	1	1	1	1	1	1	}
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0010 0010, 'Service option temporarily out of order'. Any other value received by the network shall be treated as 0110 1111, 'Protocol error, unspecified'.

NOTE: The listed reject cause values are defined in Annex G.

10.5.5.14 GMM cause

The purpose of the GMM cause information element is to indicate the reason why a GMM request from the mobile station is rejected by the network.

The GMM cause information element is coded as shown in figure 10.5.129/TS 24.008 and table 10.5.147/TS 24.008.

The GMM cause is a type 3 information element with 2 octets length.

8 7 6
5 4 3
2 1

GMM cause IEI	octet 1
Cause value	octet 2

Figure 10.5.129/TS 24.008: GMM cause information element

Table 10.5.147/TS 24.008: GMM cause information element

Cause value (octet 2) ¬

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 1 0	IMSI unknown in HLR
0 0 0 0 0 0 1 1	Illegal MS
0 0 0 0 0 1 1 0	Illegal ME
0 0 0 0 0 1 1 1	GPRS services not allowed
0 0 0 0 1 0 0 0	GPRS services and non-GPRS services not allowed
0 0 0 0 1 0 0 1	MS identity cannot be derived by the network
0 0 0 0 1 0 1 0	Implicitly detached
0 0 0 0 1 0 1 1	PLMN not allowed
0 0 0 0 1 1 0 0	Location Area not allowed
0 0 0 0 1 1 0 1	Roaming not allowed in this location area
0 0 0 0 1 1 1 1	PS MAC failure
~~0 0 0 1 1 1 1 1~~	~~PS Synch failure~~
0 0 0 1 0 0 0 0	MSC temporarily not reachable
0 0 0 1 0 0 0 1	Network failure
0 0 0 1 0 1 1 0	Congestion
0 0 1 1 0 0 0 0 to 0 0 1 1 1 1 1 1	} } retry upon entry into a new cell }
0 1 0 1 1 1 1 1	Semantically incorrect message
0 1 1 0 0 0 0 0	Invalid mandatory information
0 1 1 0 0 0 0 1	Message type non-existent or not implemented
0 1 1 0 0 0 1 0	Message type not compatible with the protocol state
0 1 1 0 0 0 1 1	Information element non-existent or not implemented
0 1 1 0 0 1 0 0	Conditional IE error
0 1 1 0 0 1 0 1	Message not compatible with the protocol state
0 1 1 0 1 1 1 1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0110 1111, 'Protocol error,' unspecified'. Any other value received by the network shall be treated as 0110 1111, 'Protocol error, unspecified'.

NOTE: The listed reject cause values are defined in Annex G.

Annex G (informative): GSM specific cause values for mobility management

This annex is informative. It describes the cause values for the mobility management procedures for non-GPRS services (MM) and GPRS services (GMM). Sections G1 to G5 are valid for both MM and GMM. However, the following codes are applicable for non-GPRS services only:

#38 Call cannot be identified

Section G.6 applies only for GMM procedures.

G.1 Causes related to MS identification

Cause value = 2 IMSI unknown in HLR

This cause is sent to the MS if the MS is not known (registered) in the HLR. This cause code does not affect operation of the GPRS service, although is may be used by a GMM procedure.

Cause value = 3 Illegal MS
This cause is sent to the MS when the network refuses service to the MS either because an identity of the MS is not acceptable to the network or because the MS does not pass the authentication check, i.e. the SRES received from the MS is different from that generated by the network.

Cause value = 4 IMSI unknown in VLR
This cause is sent to the MS when the given IMSI is not known at the VLR.

Cause value = 5 IMEI not accepted
This cause is sent to the MS if the network does not accept emergency call establishment using an IMEI.

Cause value = 6 Illegal ME
This cause is sent to the MS if the ME used is not acceptable to the network, e.g. blacklisted.

G.2 Cause related to subscription options

Cause value = 11 PLMN not allowed
This cause is sent to the MS if it requests location updating in a PLMN where the MS, by subscription or due to operator determined barring is not allowed to operate.

Cause value = 12 Location Area not allowed
This cause is sent to the MS if it requests location updating in a location area where the MS, by subscription, is not allowed to operate.

Cause value = 13 Roaming not allowed in this location area
This cause is sent to an MS which requests location updating in a location area of a PLMN which offers roaming to that MS in that Location Area, by subscription.

G.3 Causes related to PLMN specific network failures and congestion / Authentication Failures

Cause value = 7 CS MAC failure
This cause is sent to the MSC if the SIM detects that the MAC in the authentication request message is not fresh (see TS 33.102)

Cause value = 15 CS Synch failure
This cause is sent to the MSC if the SIM detects that the SQN in the authentication request message is out of range (see TS 33.102)

Cause value = 17 Network failure
This cause is sent to the MS if the MSC cannot service an MS generated request because of PLMN failures, e.g. problems in MAP.

Cause value = 22 Congestion
This cause is sent if the service request cannot be actioned because of congestion (e.g. no channel, facility busy/congested etc.)

G.4 Causes related to nature of request

Cause value = 32 Service option not supported
This cause is sent when the MS requests a service/facility in the CM SERVICE REQUEST message which is not supported by the PLMN.

Cause value = 33 Requested service option not subscribed
This cause is sent when the MS requests a service option for which it has no subscription.

Cause value = 34 Service option temporarily out of order

This cause is sent when the MSC cannot service the request because of temporary outage of one or more functions required for supporting the service.

Cause value = 38 Call cannot be identified

This cause is sent when the network cannot identify the call associated with a call re-establishment request.

G.5 Causes related to invalid messages

Cause value = 95 Semantically incorrect message.

See annex H, section H.5.10.

Cause value = 96 Invalid mandatory information.

See annex H, section H.6.1.

Cause value = 97 Message type non-existent or not implemented.

See annex H, section H.6.2.

Cause value = 98 Message not compatible with protocol state.

See annex H, section H.6.3.

Cause value = 99 Information element non-existent or not implemented

See annex H, section H.6.4.

Cause value = 100 Conditional IE error.

See annex H, section H.6.5.

Cause value = 101 Message not compatible with protocol state

See annex H, section H.6.6.

Cause value = 111 Protocol error, unspecified

See annex H, section H.6.8.

G.6 Additional cause codes for GMM

Cause value = 7 GPRS services not allowed

This cause is sent to the MS if it requests an IMSI attach for GPRS services, but is not allowed to operate GPRS services.

Cause value = 8 GPRS services and non-GPRS services not allowed

This cause is sent to the MS if it requests a combined IMSI attach for GPRS and non-GPRS services, but is not allowed to operate either of them.

Cause value = 9 MS identity cannot be derived by the network

This cause is sent to the MS when the network cannot derive the MS's identity from the P-TMSI in case of inter-SGSN routing area update.

Cause value = 10 Implicitly detached

This cause is sent to the MS either if the network has implicitly detached the MS, e.g. some while after the Mobile reachable timer has expired, or if the GMM context data related to the subscription dose not exist in the SGSN e.g. because of a SGSN restart.

Cause value = 16 MSC temporarily not reachable

This cause is sent to the MS if it requests a combined GPRS attach or routing are updating in a PLMN where the MSC is temporarily not reachable via the GPRS part of the GSM network.

Cause value = 7 PS MAC failure

This cause is sent to the SGSN if the SIM detects that the MAC in the authentication request message is not fresh (see TS 33.102)

Cause value = 15 PS Synch failure

This cause is sent to the SGSN if the SIM detects that the SQN in the authentication request message is out of range (see TS 33.102)