3GPP TSG_CN#7 **NP-000100**
ETSI SMG3 Plenary Meeting #7,
Madrid, Spain
13th – 15th March 2000

Agenda item: **5.1.3**

Source: **TSG_N WG1**

Title: **CRs to 3G Work Item Security**

Introduction:

This document contains **"12"** CRs on **Work Item Security,** that have been agreed by **TSG_N WG1,** and are forwarded to **TSG_N Plenary** meeting #7 for approval.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N1-000548	24.007	CR010	1	C	R99	3.2.0	3.3.0	Addition of integrity protection feature
N1-000475	24.008	CR155	1	C	R99	3.2.1	3.3.0	Alignment of the AUTN and Authentication Failure Parameter length
N1-000189	24.008	CR125	1	C	R99	3.2.1	3.3.0	Alignment of the procedure "Authentication not accepted by the MS" in MM and GMM.
N1-000188	24.008	CR099	1	C	R99	3.2.1	3.3.0	Authentication Reject from MS
N1-000536	24.008	CR163	1	F	R99	3.2.1	3.3.0	Clarifications on the GMM Authentication procedure
N1-000562	24.008	CR171	2	F	R99	3.2.1	3.3.0	Clarifications on the MM Authentication procedure
N1-000381	24.008	CR165		F	R99	3.2.1	3.3.0	Handling of CS keys at intersystem change
N1-000380	24.008	CR164		F	R99	3.2.1	3.3.0	Handling of GPRS keys at intersystem change
N1-000534	24.008	CR 118	3	C	R99	3.2.1	3.3.0	Integrity checking of MM and GMM messages
N1-000186	24.008	CR095	1	C	R99	3.2.1	3.3.0	UMTS security parameters, Combined reject causes for CS and PS
N1-000042	24.008	CR094		F	R99	3.2.1	3.3.0	UMTS security parameters, Correction of format for IE "Response from SIM"
N1-000041	24.008	CR093		C	R99	3.2.1	3.3.0	UMTS security parameters, Handling of Ciphering algorithm IE in UMTS

3GPP/SMG Meeting #11
Umea, Sweden, 28 February - 03 March.2000

***Document* N1-000312**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

24.007	CR	010	Current Version:	3.2.0

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

For submission to: CN#7 *list expected approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	for information		non-strategic		

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: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: CN1 **Date:** 18-02-2000

Subject: Integrity checking of signalling messages for UMTS.

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: To allow the layer 3 entities MM and GMM in the MS to be to decide whether or not to process layer 3 messages, the lower layers must indicate the result of the integrity checking procedure. The primitive RR_DATA_IND should include this.
This CR also proposes a change to the primitive RR_SYNCH_IND, to indicate to the MM/GMM layer that integrity protection is in use.

Clauses affected: 9.1.2.5, 9.1.2.7

Other specs affected:

Other 3G core specifications	X	→ List of CRs:	24.008 – CR 118r1
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.

9.1.2.5 RR_SYNC_IND

Is used for synchronizing RR and the Mobility Management entity after the establishment of a Mobile originated or Mobile terminated RR connection. This indication is provided to MM in the following cases:

- ciphering has been started (ciphering);
- integrity protection has been started (integrity) (UMTS only);
- a traffic channel has been assigned (res. ass. = "resource assigned");
- the channel mode has been modified (channel mode modify).

***** Next Modified Section *****

9.1.2.7 RR_DATA_IND

Is used by RR to indicate control-data, which has been received from its peer entity on the Network side via an existing RR connection.

For UMTS, RR_DATA_IND is also used to indicate whether control-data has been:

- successfully integrity checked;
- unsuccessfully integrity checked;
- received with no integrity protection.

3GPP CN WG1 Meeting #11
Umea, Sweden, 28/Feb-03/Mar 2000

***Document* N1-000475**
Revision of N1-000347

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	155r1	Current Version:	3.2.1

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

For submission to:	CN #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)*

(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 27/Feb/2000

Subject: Alignment of the AUTN and Authentication Failure Parameter length

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Alignment of the AUTN length is needed. Because, MODE was removed and AMF was added to the AUTN in the 33.102.
Alignment of the Response from SIM(renamed to Authentication Failure parameter) length that still has wrong length is needed.

Clauses affected: 9.2.2, 9.2.3a, 9.4.9, 9.4.10a, 10.5.3.1.2, 10.5.3.2.2

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: Other necessary alignments were done by N1-000188.


help.doc

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

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	16~~4~~-20~~19~~

********** NEXT MODIFICATION **********

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 9.2.4a/TS 24.008.

Message type: CS AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.2.4a/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	14~~30~~ - 18~~32~~

********** NEXT MODIFICATION **********

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/GSM 24.008.

Message type: AUTHENTICATION AND CIPHERING REQUEST

Significance: dual

Direction: network to MS

Table 9.4.9/GSM 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
	A&C reference number	A&C reference number 10.5.5.19	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	16~~4~~ 20~~19~~

********** NEXT MODIFICATION **********

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	14~~30~~ - 18~~32~~

********** NEXT MODIFICATION **********

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 16~~4~~ octets and a maximum of 20~~19~~ octets length.

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

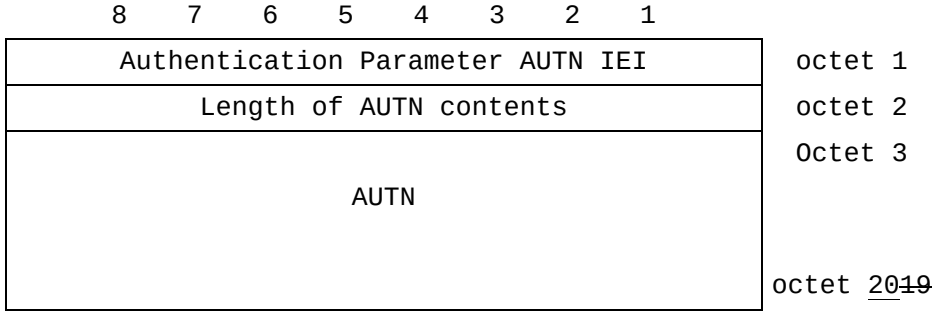

Table 10.5.89.1/TS 24.008 *Authentication Parameter AUTN* information element (UMTS authentication challenge only)

AUTN value (octets 3 to 20~~19~~) The AUTN consists of (SQN xor AK)||AMF~~MODE~~||MAC =(32 to 64)+16~~1~~+64 bits (see TS 33.102)

********** NEXT MODIFICATION **********

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 14~~30~~ octets and a maximum length of 18~~32~~ octets.

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

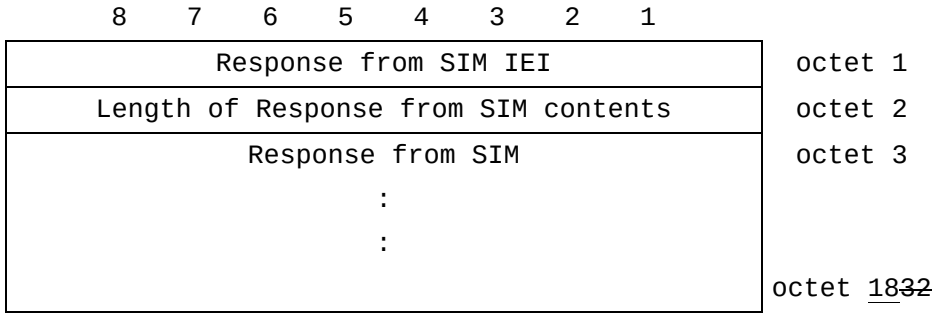

Table 10.5.90.2/TS 24.008: *Response from SIM* information element

Response from SIM value (octet 3 to 18~~32~~) This contains $RAND_{MS}$ and AUTS (see TS 33.102)

3GPP CN1 Meeting #10
Abiko, Japan, 11 – 14 Jan 2000

Document N1-000189
revised N1-000134

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	125r1	Current Version:	3.2.1

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

For submission to:	TSG N #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 13-Jan-2000

Subject: Alignment of the procedure “Authentication not accepted by the MS” in MM and GMM.

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: CR of Adaptation of MM and GMM messages to incorporate UMTS security parameters (N1-99E95) was approved in Bad Aibling meeting.
This CR is to add the process that the core network stops the timer T3260 in 4.3.2.5.1 Authentication not accepted by the MS and stops the timer T3360 in 4.7.7.5.1 Authentication not accepted by the MS.

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.

4.3.2.3 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).
Upon receipt of the AUTHENTICATION FAILURE message, the network stops the timer T3260. In MAC failure case, the procedural behaviour is ffs. In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

******* ***Next Modification*** *******

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.

GMM

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, 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]).
Upon receipt of the AUTHENTICATION AND CIPHERING FAILURE message, the network stops the timer T3360. In MAC failure case, the procedural behaviour is ffs. In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

******* ***Next Modification*** *******

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.

****** Next Modification ******

11.2 Timers of mobility management

Table 11.1/TS 24.008: Mobility management timers - MS-side

TIMER NUM.	MM STAT	TIME OUT VAL.	CAUSE FOR START	NORMAL STOP	AT THE EXPIRY
T3210	3	20s	-LOC_UPD_REQ sent	- LOC_UPD_ACC - LOC_UPD_REJ - AUTH_REJ - Lower layer failure	Start T3211
T3211	1 2	15s	-LOC_UPD_REJ with cause #17 netw. failure -lower layer failure or RR conn. released after RR conn. abort during loc. updating	- Time out - cell change - request for MM connection establishment - change of LA	Restart the Location update proc.
T3212	1, 2	Note 1	-termination of MM service or MM signalling	-initiation of MM service or MM signalling	initiate periodic updating
T3213	1 2 11	4s	-location updating failure	- expiry - change of BCCH parameter	new random attempt
T3220	7	5s	-IMSI DETACH	- release from RM-sublayer	enter Null or Idle, ATTEMPTING TO UPDATE
T3230	5	15s	-CM SERV REQ CM REEST REQ	- Cipher mode setting - CM SERV REJ - CM SERV ACC	provide release ind.
T3240	9 10	10s	see section 11.2.1	see section 11.2.1	abort the RR connection

NOTE 1: The timeout value is broadcasted in a SYSTEM INFORMATION message

Table 11.2/TS 24.008: Mobility management timers - network-side

TIMER NUM.	MM ST AT	TIME OUT VAL.	CAUSE FOR START	NORMAL STOP	AT THE FIRST EXPIRY	AT THE SECOND EXPIRY
T3250	6	12s	TMSI-REAL-CMD or LOC UPD ACC with new TMSI sent	TMSI-REALL-COM received	Optionally Release RR connec-tion	
T3255		Note	LOC UPD ACC sent with "Follow on Proceed"	CM SERVICE REQUEST	Release RR Connection or use for mobile sta-tion termi-nating call	
T3260	5	12s	AUTHENT-REQUEST sent	AUTHENT-RESPONSE received	Optionally Release RR connec-tion	
				AUTHENT-FAILURE received	Procedural behavior is FFS	
T3270	4	12s	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Optionally Release RR connec-tion	

NOTE 2: The value of this timer is not specified by this recommendation.

11.2.1 Timer T3240

Timer T3240 is started in the mobile station when:

- the mobile station receives a LOCATION UPDATING ACCEPT message completing a location updating procedure in the cases specified in section 4.4.4.6 and 4.4.4.8;
- the mobile station receives a LOCATION UPDATING REJECT message in the cases specified in section 4.4.4.7;
- the mobile station has sent a CM SERVICE ABORT message as specified in section 4.5.1.7;
- the mobile station has released or aborted all MM connections in the cases specified in 4.3.2.5, 4.3.5.2, 4.5.1.1, and 4.5.3.1.

Timer T3240 is stopped, reset, and started again at receipt of an MM message.
Timer T3240 is stopped and reset (but not started) at receipt of a CM message that initiates establishment of an CM connection (an appropriate SETUP, REGISTER, or CP-DATA message as defined in TS 24.008, TS 24.010 or GSM 04.11).

11.2.2 Timers of GPRS mobility management

Table 11.3/TS 24.008: GPRS Mobility management timers - MS side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY Note 3
T3310	15s	GMM-REG-INIT	ATTACH REQ sent	ATTACH ACCEPT received ATTACH REJECT received	Retransmission of ATTACH REQ
T3311	15s	GMM-DEREG ATTEMPTING TO ATTACH or GMM-REG ATTEMPTING TO UPDATE	ATTACH REJ with other cause values as described in chapter 'GPRS Attach' ROUTING AREA UPDATE REJ with other cause values as described in chapter 'Routing Area Update' Low layer failure	Change of the routing area	Restart of the Attach or the RAU procedure with updating of the relevant attempt counter
T3321	15s	GMM-DEREG-INIT	DETACH REQ sent	DETACH ACCEPT received	Retransmission of the DETACH REQ
T3330	15s	GMM-ROUTING-UPDATING-INITIATED	ROUTING AREA UPDATE REQUEST sent	ROUTING AREA UPDATE ACC received ROUTING AREA UPDATE REJ received	Retransmission of the ROUTING AREA UPDATE REQUEST message

Table 11.3a/TS 24.008: GPRS Mobility management timers – MS side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3302	T3212 Note 4	GMM-DEREG or GMM-REG	At attach failure and the attempt counter is greater than or equal to 5. At routing area updating failure and the attempt counter is greater than or equal to 5.	At successful attach At successful routing area updating	On every expiry, initiation of the GPRS attach procedure or RAU procedure
T3312	Default 54 min Note1	GMM-REG	In GSM, when READY state is left. In UMTS, when PMM-CONNECTED mode is left.	When entering state GMM-DEREG	Initiation of the Periodic RAU procedure
T3314 READY (GSM only)	Default 44 sec Note 2	All except GMM-DEREG	Transmission of a PTP PDU	Forced to Standby	No cell-updates are performed
T3316 AA-READY	Default 44 sec Note 2	-	Transmission of a PTP PDU	-	-
T3317 (UMTS only)	10s	GMM-REG	SERVICE REQ sent	Security mode setting procedure is completed, SERVICE ACCEPT received, or SERVICE REJECT received	Abort the procedure

NOTE 1: The value of this timer is used if the network does not indicate another value in a GMM signalling procedure.

NOTE 2: The default value of this timer is used if neither the MS nor the Network send another value, or if the Network sends this value, in a signalling procedure.

NOTE 3: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

NOTE 4: T3302 is loaded with the same value which is used to load T3212.

Table 11.4/TS 24.008: GPRS Mobility management timers - network side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY Note 3
T3322	6s	GMM-DEREG-INIT	DETACH REQ sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST
T3350	6s	GMM-COMMON-PROC-INIT	ATTACH ACCEPT sent with P-TMSI and/or TMSI RAU ACCEPT sent with P-TMSI and/or TMSI P-TMSI REALLOC COMMAND sent	ATTACH COMPLETE received RAU COMPLETE received P-TMSI REALLOC COMPLETE received	Retransmission of the same message type, i.e. ATTACH ACCEPT, RAU ACCEPT or REALLOC COMMAND
T3360	6s	GMM-COMMON-PROC-INIT	AUTH AND CIPH REQUEST sent	AUTH AND CIPH RESPONSE received AUTHENT- AND CIPHER- FAILURE received	Retransmission of AUTH AND CIPH REQUEST Procedural behaviour is FFS
T3370	6s	GMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQUEST

Table 11.4a/TS 24.008: GPRS Mobility management timers - network side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3313	Note1	GMM_REG	Paging procedure initiated	Paging procedure completed	Network dependent
T3314 READY (GSM only)	Default 44 sec Note 2	All except GMM-DEREG	Receipt of a PTP PDU	Forced to Standby	The network shall page the MS if a PTP PDU has to be sent to the MS
T3316 AA-READY	Default 44 sec Note 2	-	Receipt of a PTP PDU	-	-
Mobile Reachable	Default 4 min greater than T3312	All except GMM-DEREG	In GSM, change from READY to STANDBY state In UMTS, change from PMM-CONNECTED mode to PMM-IDLE mode.	PTP PDU received	Network dependent but typically paging is halted on 1st expiry

NOTE 1: The value of this timer is network dependent.

NOTE 2: The default value of this timer is used if neither the MS nor the Network send another value, or if the Network sends this value, in a signalling procedure. The value of this timer should be slightly shorter in the network than in the MS, this is a network implementation issue.

NOTE 3: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

3GPP/SMG TSG-CN WG1 Meeting #9
Abiko, Japan, 11-15 Jan 2000

Document* *N1-000188
Rev. of N1-000070

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**	**099r1**	Current Version:	3.2.1

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

For submission to: TSG CN #7 (*list expected approval meeting # here ↑*)

for approval [X]
for information [ ]

strategic [ ]
non-strategic [ ]
(for SMG 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: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: CN1 **Date:** 2000-01-13

Subject: Authentication Reject from MS

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	[ ]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change:

This CR proposes to rename the signalling name 'CS Authentication failure' to 'Authentication Failure' and 'PS Authentication failure' to 'Authentication and Ciphering Failure' defined in the MS -> network direction.

The requirement for the MS to include the parameter $RAND_{MS}$ in the AUTHENTICATION FAILURE messages has been removed in new version of 33.102.

The Response from SIM IE is renamed to Authentication Failure parameter IE.

Clauses affected: 4.3.2.5.1, 4.7.7.5.1, 9.2.3a, 9.4.10a, 10.4, 10.5.3.2.2

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.

4.3.2.5.1 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 TS 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.

***** Next Modification *****

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 AND CIPHERING 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 AND CIPHERING FAILURE message ~~(9.2.3a)~~ to the network, with the failure cause 'PS Synch failure' and parameters provided by the SIM (see TS 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.

***** Next Modification *****

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 9.2.4a/TS 24.008.

Message type:~~CS~~ AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.2.4a/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~~Authentication Failure parameter	~~Response from SIM~~Authentication Failure parameter 10.5.3.2.2	O	TLV	~~30~~14 - ~~32~~16

9.2.3a.1 ~~Response from SIM~~Authentication Failure parameter

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 parameter~~s~~ (see TS 33.102).

***** Next Modification *****

9.4.10a~~PS~~ Authentication and Ciphering 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 AND CIPHERING FAILURE

Significance: dual

Direction: mobile station to network

Table 9.4.10a/TS 24.008: ~~PS~~ AUTHENTICATION AND CIPHERING 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 and Ciphering 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~~Authentication Failure parameter	~~Response from SIM~~Authentication Failure parameter 10.5.3.2.2	O	T	~~30~~14 ~~–~~ ~~32~~16

9.4.10a.1 ~~Response from SIM~~Authentication Failure parameter

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 parameter~~s~~ (see TS 33.102).

***** Next Modification *****

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	
x	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
x	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
x	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
x	x	1	1	-	-	-	-	Miscellaneous messages:
				0	0	0	0	- MM NULL
				0	0	0	1	- MM STATUS
				0	0	1	0	- MM INFORMATION

When the radio connection started with a core network node of earlier than R99, bit 8 shall be set to 0 and bit 7 is reserved for the send sequence number in messages sent from the mobile station. In messages sent from the network, bits 7 and 8 are coded with a "0". See TS 24.007.
When the radio connection started with a core network node of R’99 or later, bits 7 and 8 are reserved for the send sequence number in messages sent from the mobile station. In messages sent from the network, bits 7 and 8 are 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 0 1 1 0 0	Service Request
0 0 0 0 1 1 0 1	Service Accept
0 0 0 0 1 1 1 0	Service 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 and ciphering ~~F~~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

***** Next Modification *****

10.5.3.2.2 ~~Response from SIM~~Authentication Failure parameter (UMTS authentication challenge only)

The purpose of the ~~*Response from SIM*~~ *Authentication Failure parameter* 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~~Authentication Failure parameter 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~~Authentication Failure parameter IE is a type 4 information element with a minimum length of ~~30~~14 octets and a maximum length of ~~32~~16 octets.

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

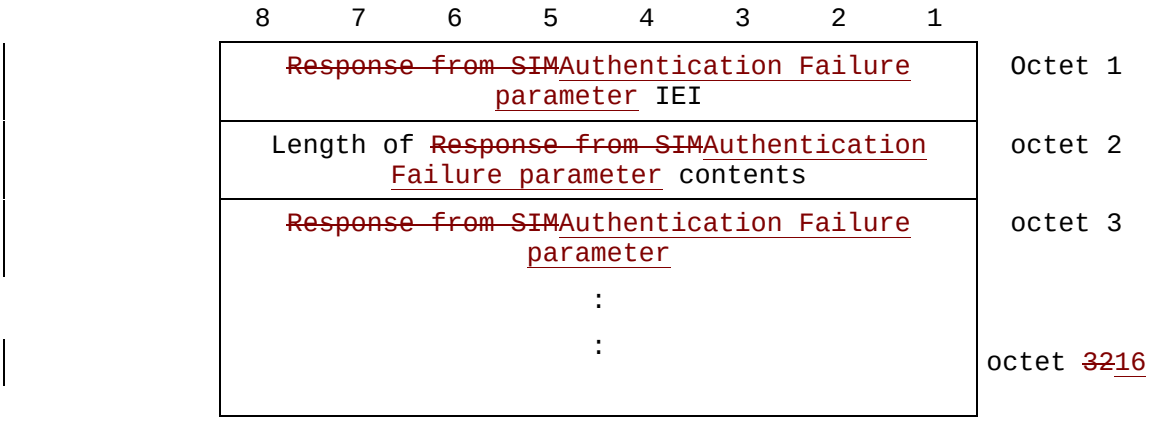

Table 10.5.90.2/TS 24.008: ~~*Response from SIM*~~Authentication Failure parameter information element

~~Response from SIM~~Authentication Failure parameter value (octet 3 to 16~~32~~)
This contains ~~$RAND_{MS}$ and~~ AUTS (see TS 33.102)

3GPP/SMG TSG-CN WG1 Meeting #11
Umeå, Sweden, 28 Feb – 03 Mar 2000

***Document* N1-000536**
Rev of ***N1-000379***

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	163r1	Current Version:	3.2.1

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

For submission to:	TSG CN #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 2000-02-20

Subject: Clarifications on the GMM Authentication procedure

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change: Some clarifications and editorial changes are needed for the GMM authentication procedure, e.g. start of ciphering is dependent on radio access system, the calculated security key(s) is dependent on the type of performed authentication

Clauses affected: 4.1.3.2, 4.7.7

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:

4.1.3.2 GPRS update status

In addition to the GMM sublayer states described so far, a GPRS update status exists.
The GPRS update status pertains to a specific subscriber embodied by a SIM. This status is defined even when the subscriber is not activated (SIM removed or connected to a switched off ME). It is stored in a non volatile memory in the SIM. The GPRS update status is changed only after execution of a GPRS attach, network initiated GPRS detach, authentication procedure, or routing area updating procedure.

GU1: UPDATED

The last GPRS attach or routing area updating attempt was successful (correct procedure outcome, and the answer was accepted by the network). The SIM contains the RAI of the routing area (RA) to which the subscriber was attached, and possibly a valid P-TMSI, GPRS GSM ciphering key, GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS ciphering key sequence number.

GU2: NOT UPDATED

The last GPRS attach or routing area updating attempt failed procedurally, i.e. no response was received from the network. This includes the cases of failures or congestion inside the network.

In this case, the SIM may contain the RAI of the routing area (RA) to which the subscriber was attached, and possibly also a valid P-TMSI, GPRS GSM ciphering key, GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS ciphering key sequence number. For compatibility reasons, all these fields shall be set to the "deleted" value if the RAI is deleted. However, the presence of other values shall not be considered an error by the MS.

GU3: ROAMING NOT ALLOWED

The last GPRS attach or routing area updating attempt was correctly performed, but the answer from the network was negative (because of roaming or subscription restrictions).

For this status, the SIM does not contain any valid RAI, P-TMSI, GPRS GSM ciphering key, GPRS UMTS ciphering key, GPRS UMTS integrity key or GPRS ciphering key sequence number. For compatibility reasons, all these fields must be set to the value "deleted" at the moment the status is set to ROAMING NOT ALLOWED. However, the presence of other values shall not be considered an error by the MS.

***** Next Modification *****

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 TS 33.102~~GSM 03.20 [13]~~);
- to provide parameters enabling the MS to calculate a new GPRS UMTS ciphering key and a new GPRS UMTS integrity key~~sequence number~~.
- to let the network set the ~~security~~ GSM ciphering mode (ciphering ~~security~~/no ciphering ~~security~~) and GSM ciphering algorithm; and
- ~~T~~to permit the ~~receiving entity~~ mobile station to ~~check the integrity of signalling messages~~ authenticate the network.

~~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.~~ UMTS authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

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

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

In GSM, the network should not send any user data during the authentication and ciphering procedure.

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

4.7.7b Authentication and ciphering procedure used for GSM authentication challenge

The purpose of the authentication and ciphering procedure is threefold:

- 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 GSM ciphering key; and
- ~~In GSM,~~ to let the network set the GSM ciphering mode (ciphering/no ciphering) and GSM ciphering algorithm.

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

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

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

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

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

GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

In GSM, ~~T~~the network should not send any user data during the authentication and ciphering procedure.

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

4.7.7.1 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] and TS 33.102).
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 GSM ciphering key and the RAND, or

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

In GSM, 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 nor the AUTN.

In GSM, if ciphering is requested in a GSM authentication challenge or in a UMTS authentication challenge, then the AUTHENTICATION AND CIPHERING REQUEST message shall indicate the GPRS GSM 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

In GSM, ~~A~~an MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time.

In UMTS, an MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time whilst a PS signalling connection exists.

In a GSM authentication challenge, 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. A GSM authentication challenge will result in the SIM passing a SRES and a GPRS GSM ciphering key to the ME. The new GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous one and any previously stored GPRS UMTS ciphering and GPRS UMTS integrity keys shall be deleted. ~~It~~The calculated GSM ciphering key shall be stored on the SIM~~and shall be loaded into the ME~~ together with the GPRS ciphering key sequence number 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, 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 verifies the AUTN parameter and if this is accepted, 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. A UMTS authentication challenge will result in the SIM passing a RES, a GPRS UMTS ciphering key, a GPRS UMTS integrity key and a GPRS GSM ciphering key to the ME. The new GPRS UMTS ciphering key~~s~~, GPRS UMTS integrity key and GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous ones ~~and~~ . The new GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS GSM ciphering key shall be stored on the SIM together with the GPRS ciphering key

sequence number before the AUTHENTICATION AND CIPHERING 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 neither the GSM~~PRS~~ authentication parameters (RAND and GPRS CKSN) nor the UMTS authentication parameters (~~RAND and GPRS CKSN or~~ 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, the GMM layer shall notify the LLC layer if ciphering shall be used or not and if yes which GSM ciphering algorithm and GPRS GSM 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] and TS 33.102). 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, the GMM layer shall notify the LLC sublayer if ciphering shall be used or not and if yes which algorithm and GPRS GSM 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~~. In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter SRES and the GPRS GSM 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 RES and the GPRS UMTS ciphering key and the GPRS UMTS integrity 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 GPRS ciphering key sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the GPRS ciphering key sequence number allocated to the GPRS GSM ciphering key (in case of a GSM authentication challenge) or the GPRS UMTS ciphering key and the GPRS UMTS integrity key~~(s)~~ (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.

The MS stores the~~is~~ GPRS ciphering key sequence number with the GPRS GSM ciphering key (in case of a GSM authentication challenge) and the GPRS UMTS ciphering key and the GPRS UMTS integrity key ~~(s)~~ (in case of a UMTS authentication challenge), and includes the corresponding GPRS ciphering key sequence number in the ROUTING AREA UPDATE REQUEST, SERVICE REQUEST and ATTACH REQUEST messages.

If the GPRS ciphering key sequence number is deleted, the associated GPRS GSM ciphering key~~(s)~~, GPRS UMTS ciphering key and GPRS UMTS integrity key shall be ~~considered as invalid~~deleted (i.e. the established GSM security context or the UMTS security context is no longer valid).

In UMTS, the network may choose to start ciphering and integrity checking with the stored GPRS UMTS ciphering key and the stored GPRS UMTS integrity key (under the restrictions given in GSM 02.09 and TS 33.102) if the stored GPRS ciphering key sequence number and the one given from the MS are equal.

In GSM, ~~T~~the network may choose to start ciphering with the stored GPRS GSM ciphering key (under the restrictions given in GSM 02.09) if the stored GPRS ciphering key 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, the MS starts ciphering after sending the AUTHENTICATION AND CIPHERING RESPONSE message. The networkSGSN starts ciphering when a valid AUTHENTICATION AND CIPHERING RESPONSE is received from the MS.

In UMTS, the MS starts ciphering and integrity checking according to the conditions specified in see specification TS 25.331.
In GSM, 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 networkSGSN 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.

NOTE: In some specifications the term KSI (Key Set Identifier) is used instead of the term GPRS ciphering key sequence number.

4.7.7.5 Authentication not accepted by the network

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.

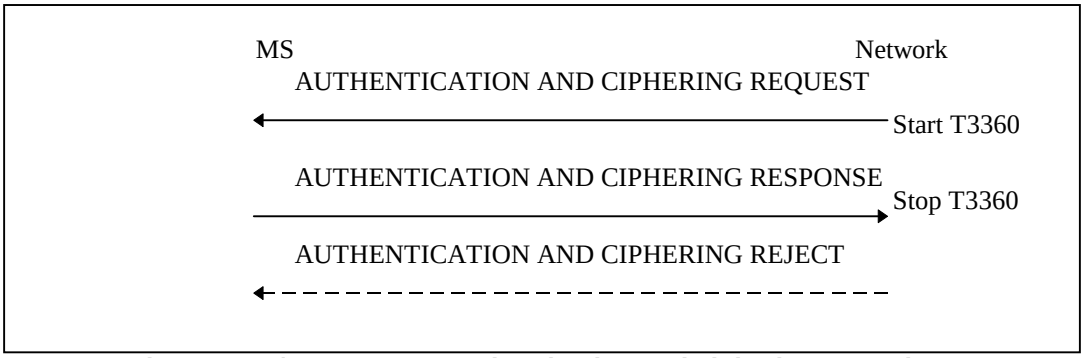

Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

4.7.7.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102.

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331).

NOTE: In UMTS, during an ongoing, already ciphering/integrity protected PS signalling connection, the network might initiate a new Authentication and ciphering procedure in order to establish a new GSM/UMTS security context. The new GPRS UMTS ciphering key and GPRS UMTS integrity key are taken into use by the MS, when a new valid SECURITY MODE COMMAND indicating PS domain is received during the PS signalling connection.

3GPP/SMG TSG-CN WG1 Meeting #11
Umeå, Sweden, 28 Feb – 03 Mar 2000

Document N1-000562
Rev of N1-000535

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	171r2	Current Version:	3.2.1

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

For submission to: TSG CN #7 (*list expected approval meeting # here ↑*)

for approval [X] for information [ ]

strategic [ ] non-strategic [ ] *(for SMG 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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: CN1 **Date:** 2000-02-20

Subject: Clarifications on the MM Authentication procedure

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change: Some clarifications and editorial changes are needed for the MM authentication procedure, e.g. start of ciphering is dependent on radio access system, the calculated security key(s) is dependent on the type of performed authentication

Clauses affected: 2.2.2, 4.1.2.2, 4.1.2.3, 4.3.2

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:

2.2.2 Vocabulary

The following terms are used in this Technical Specification:

- A **GSM security context** is established and stored in the MS and the network as a result of a successful execution of a GSM authentication challenge. The GSM security context consists of the GSM ciphering key and the ciphering key sequence number.

- A **UMTS security context** is established and stored in the MS and the network as a result of a successful execution of a UMTS authentication challenge. The UMTS security context consists of the UMTS ciphering key, the UMTS integrity key, the GSM ciphering key and the cipher key sequence number.

***** Next Modification *****

4.1.2.2 The update Status

In parallel with the sublayer states described in section 4.1.2.1 and which control the MM sublayer protocol, an update status exists.
The update status pertains to a specific subscriber embodied by a SIM. This status is defined even when the subscriber is not activated (SIM removed or connected to a switched-off ME). It is stored in a non volatile memory in the SIM. The update status is changed only as a result of a location updating procedure attempt (with the exception of an authentication failure and of some cases of CM service rejection). In some cases, the update status is changed as a result of a GPRS attach, GPRS routing area update, service request or network initiated GPRS detach procedure.

U1 UPDATED

The last location updating attempt was successful (correct procedure outcome, and the answer was acceptance from the network). With this status, the SIM contains also the LAI of the LA where the subscriber is registered, and possibly valid TMSI, GSM ciphering key, UMTS integrity key, UMTS ciphering key and ciphering key sequence number. The "Location update status" stored on the SIM shall be "updated".

U2 NOT UPDATED

The last location updating attempt made failed procedurally (no significant answer was received from the network, including the cases of failures or congestion inside the network).

For this status, the SIM does not contain any valid LAI, TMSI, GSM ciphering key, UMTS integrity key, UMTS ciphering key or ciphering key sequence number. For compatibility reasons, all these fields must be set to the "deleted" value at the moment the status is set to NOT UPDATED. However the presence of other values shall not be considered an error by the mobile station. The "Location update status" stored on the SIM shall be "not updated".

U3 ROAMING NOT ALLOWED

The last location updating attempt run correctly, but the answer from the network was negative (because of roaming or subscription restrictions).

For this status, the SIM does not contain any valid LAI, TMSI, GSM ciphering key, UMTS integrity key, UMTS ciphering key or ciphering key sequence number. For compatibility reasons, all these fields must be set to the "deleted" value at the moment the status is set to ROAMING NOT ALLOWED. However the presence of other values shall not be considered an error by the mobile station. The "Location update status" stored on the SIM shall be "Location Area not allowed".

***** Next Modification *****

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. SECURITY MODE INITIATED

In UMTS, ~~The~~ the security mode setting procedure has been requested to the RR sublayer.

In GSM, the cipher 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.

***** Next Modification *****

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~~TS 33.102);

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

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

Fourth to permit the ~~receiving entity~~ mobile station to ~~check the integrity of the network~~ authenticate 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. UMTS authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

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

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 GSM 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. GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

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

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 (in case of GSM authentication challenge) and TS 33.102 (in case of an UMTS authentication challenge)). In a GSM authentication challenge, ~~It~~ the AUTHENTICATION REQUEST message also contains the ciphering key~~(s)~~ sequence number allocated to the GSM ciphering key which may be computed from the given parameters. In a UMTS authentication challenge, the AUTHENTICATION REQUEST message also contains the ciphering key sequence number allocated to the key set of UMTS ciphering key, UMTS integrity key and GSM ciphering key 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. With exception of the cases described in 4.3.2.5.1, ~~I~~it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

In a GSM authentication challenge, ~~T~~the new GSM ciphering key ~~(GSM authentication challenge)~~ calculated from the challenge information shall overwrite the previous GSM ciphering key and any previously stored UMTS ciphering key and UMTS integrity key shall be deleted. The new GSM ciphering key shall be stored on the SIM together with the ciphering key sequence number.

In a UMTS authentication challenge, ~~or~~ the new UMTS ciphering key, the new GSM ciphering key and the new UMTS integrity key ~~(UMTS authentication challenge)~~ calculated from the challenge information shall overwrite the previous UMTS ciphering key, GSM ciphering key and UMTS integrity key ~~one(s) .~~ ~~and~~ The new UMTS ciphering key, GSM ciphering key and UMTS integrity key are ~~be~~ stored on the SIM together with the ciphering key sequence number ~~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 SECURITY MODE COMMAND is received during an RR connection (the definition of a valid 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~~A UMTS authentication challenge will result in the SIM passing a RES, a UMTS ~~C~~ciphering ~~K~~key, ~~and an~~ a UMTS ~~I~~integrity ~~K~~key to the ME~~mobile station~~. A GSM authentication challenge will result in the SIM passing a SRES and a GSM ~~C~~ciphering ~~K~~key to the ME~~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 in case of a GSM authentication challenge respective TS 33.102 in case of an UMTS authentication challenge).

4.3.2.4 Ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets.In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter SRES and the GSM 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 RES and the UMTS ciphering key and the UMTS 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 ciphering key sequence number is managed by the network in the way that the AUTHENTICATION REQUEST message contains the ciphering key sequence number allocated to the GSM ciphering key~~(s)~~ (in case of a GSM authentication challenge) or the UMTS ciphering key and the UMTS integrity key (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.
The mobile station stores the~~is~~ ciphering key sequence number with the GSM ciphering key~~(s),~~ (in case of a GSM authentication challenge) and the UMTS ciphering key and the UMTS integrity key (in case of a UMTS authentication challenge) and indicates to the network in the first message (LOCATION UPDATING

REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST) which ciphering key sequence number the stored GSM ciphering key (in case of a GSM authentication challenge) or set of UMTS ciphering and UMTS integrity keys (in case of a UMTS authentication challenge) has.

When the deletion of the ciphering key sequence number is described this also means that the associated GSM ciphering key~~(s)~~, the UMTS ciphering key and the UMTS integrity key shall be considered as invalid (i.e. the established GSM security context or the UMTS security context is no longer valid).

In GSM, ~~T~~the network may choose to start ciphering with the stored GSM ciphering key~~(s)~~ (under the restrictions given in GSM 02.09) if the stored ciphering key sequence number and the one given from the mobile station are equal.

In UMTS, the network may choose to start ciphering and integrity with the stored UMTS ciphering key and UMTS integrity key (under the restrictions given in GSM 02.09 and TS 33.102) if the stored ciphering key sequence number and the one given from the mobile station are equal.

NOTE: In some specifications the term KSI (Key Set Identifier) might be used instead of the term ciphering key sequence number.

4.3.2.5 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 of 04.18 (GSM) or in TS 25.331 (UMTS).
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 GSM~~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.

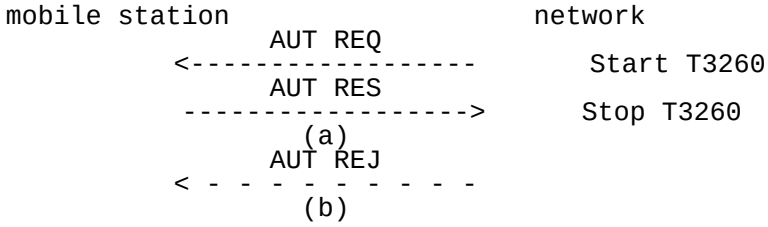

Figure 4.2/TS 24.008: Authentication sequence: (a) authentication; (b) authentication rejection.

4.3.2.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in GSM 04.18 section 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in GSM 04.18 section 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named "c3" defined in TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102. The derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102.

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331).

NOTE: In UMTS and GSM, during an ongoing, already ciphering and/or integrity protected RR connection, the network might initiate a new Authentication procedure in order to establish a new GSM/UMTS security context. The new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection.

3GPP/TSG-CN-WG1, Meeting #11
Umea, Sweden, 28.2. – 2.3.2000

***Document* N1-000381**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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	165	Current Version:	3.2.1

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

For submission to:	CN#7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: CN1 **Date:** 2000-02-21

Subject: Handling of CS keys at intersystem change

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: A description of the appropriate security keys for the MS to apply after intersystem change between GSM and UMTS is needed to allow continued ciphering (and integrity for UMTS) without any new authentication.

Clauses affected: 4.3.2.7 (new section), 4.3.2.8 (new section)

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:

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At intersystem change from UMTS to GSM, ciphering may be started (see GSM 04.18) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to Table 4.3.2.7.1.

Table 4.3.2.7.1/TS 24.008: Intersystem change from UMTS to GSM

Security context established in MS and network in UMTS	At intersystem change to GSM:
GSM security context	An ME shall apply the GSM cipher key received from the GSM security context residing in the SIM.
UMTS security context	An ME shall apply the GSM cipher key derived by the SIM from the UMTS cipher key and the UMTS integrity key.

NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At intersystem change from UMTS to GSM, ciphering and integrity may be started (see TS 25.331) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to Table 4.3.2.8.1.

Table 4.3.2.8.1/TS 24.008: Intersystem change from GSM to UMTS

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and UMTS integrity key from the GSM cipher key provided by the SIM. The conversion functions named “c4” and “c5” in TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the UMTS ciphering key and the UMTS integrity key received from the UMTS security context residing in the SIM.

NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

3GPP/TSG-CN-WG1, Meeting #11
Umea, Sweden, 28.2. – 2.3.2000

***Document* N1-000380**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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	164	Current Version:	3.2.1

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

For submission to:	CN#7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 2000-02-22

Subject: Handling of GPRS keys at intersystem change

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: A description of the appropriate security keys for the MS to apply after intersystem change between GSM and UMTS is needed to allow continued ciphering (and integrity for UMTS) without any new authentication.

Clauses affected: 4.7.7.7 (new section), 4.7.7.8 (new section)

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:

4.7.7.7 Handling of keys at intersystem change from UMTS to GSM

At an intersystem change from UMTS to GSM, ciphering may be started (see GSM 04.64 [76]) without any new authentication and ciphering procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS GSM ciphering key according to Table 4.7.7.7.1.

Before any initial GMM message is sent in the new cell in GSM, the GMM layer in the MS shall notify the LLC layer if ciphering shall be used or not. If yes, the GPRS GSM ciphering key and the applicable ciphering algorithm according to the stored *Ciphering Algorithm IE* in the MS shall also be indicated to the LLC layer (see GSM 04.64 [76]).

Table 4.7.7.7.1/TS 24.008: Intersystem change from UMTS to GSM

Security context established in MS and network in UMTS	At intersystem change to GSM:
GSM security context	An ME shall apply the GPRS GSM cipher key received from the GSM security context residing in the SIM.
UMTS security context	An ME shall apply the GPRS GSM cipher key derived by the SIM from the GPRS UMTS cipher key and the GPRS UMTS integrity key.

NOTE A SIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.

4.7.7.8 Handling of keys at intersystem change from GSM to UMTS

At an intersystem change from GSM to UMTS, ciphering and integrity may be started (see TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to Table 4.7.7.8.1.

Table 4.7.7.8.1/TS 24.008: Intersystem change from GSM to UMTS

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and GPRS UMTS integrity key from the GPRS GSM cipher key provided by the SIM. The conversion functions named “c4” and “c5” in TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the GPRS UMTS ciphering key and the GPRS UMTS integrity key received from the UMTS security context residing in the SIM.

NOTE A SIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.

3GPP/SMG Meeting #11
Umea, Sweden, 28 February – 03 March.2000

Document N1-000534
(previously N1-000476)

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	118r3	Current Version:	3.2.1

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

For submission to:	CN #7	for approval	X	Strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: CN1 **Date:** 15/02/2000

Subject: Integrity checking of MM and GMM messages

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change:

It is a requirement of UMTS that signalling messages be integrity protected. This protection allows the receiving entity to be sure that the messages are from a genuine source, and thus guards against 'replay attacks.'
All protocols shall use integrity protection, and integrity protection is mandatory even in networks where encryption is not turned on.

The receiving entity (MS or RNC) uses a secret key, obtained from and known only by the SIM and the HLR/Auc, to check the integrity 'signature' of a message. Lower layers are responsible for carrying out such checks and, in general, every signalling message received will be discarded by the lower layers if it does not pass the check. However, there are certain messages in MM/GMM that should be allowed up to the layer 3 entity, without having been successfully checked. (This may be because no keys have been agreed yet, or because ciphering and integrity has not been activated yet). On the other hand, there is also a case where, in a network which does not use encryption, certain messages must never be processed at layer 3 unless they have been successfully integrity checked.

Therefore, it is necessary in MM/GMM to run integrity checking almost on a per-message basis.

Clauses affected: 4.1.1.1

Other specs affected:

Other 3G core specifications	X	→ List of CRs:	24.007 – CR010
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.

Elementary procedures for Mobility Management

4.1 General

This section describes the procedures used for mobility management for non-GPRS services and for GPRS-services at the radio interface (Reference Point Um and Uu).

The main function of the Mobility Management sublayer is to support the mobility of user terminals, such as informing the network of its present location and providing user identity confidentiality.

A further function of the MM sublayer is to provide connection management services to the different entities of the upper Connection Management (CM) sublayer (see TS 24.007).

There are two sets of procedures defined in this chapter:

- MM procedures for non-GPRS services (performed by the MM entity of the MM sublayer); and
- GMM procedures for GPRS services (performed by the GMM entity and GMM-AA entity of the MM sublayer), see TS 24.007 [20].

All the MM procedures described in this section can only be performed if a RR connection has been established between the MS and the network. Else, the MM sublayer has to initiate the establishment of a RR connection (see GSM 04.18 section 3.3 and TS 25.331 section 8.2.3). The GMM procedures described in this section, use services provided by the RR sublayer without prior RR connection establishment.

GMM procedures are mandatory and applicable only for GPRS MSs and networks supporting those MSs. For GPRS MSs which are IMSI attached for both GPRS and non-GPRS services, some MM procedures are replaced by GMM combined procedures provided that the network operates in network operation mode I, i.e. is supporting combined GMM procedures. GMM combined procedures are not applicable for the GPRS MS operation mode C but are mandatory for the GPRS MS operation modes A and B and networks supporting network operation mode I, see TS 23.060.

4.1.1 MM and GMM procedures

4.1.1.1 Types of MM and GMM procedures

Depending on how they can be initiated, three types of MM procedures can be distinguished:

1) MM common procedures:

   A MM common procedure can always be initiated whilst a RR connection exists. The procedures belonging to this type are:

   Initiated by the network:

   - TMSI reallocation procedure;
   - authentication procedure;
   - identification procedure;
   - MM information procedure;
   - abort procedure.

     However, abort procedure is used only if an MM connection is being established or has already been established i.e. not during MM specific procedures or during IMSI detach procedure, see section 4.3.5.

   Initiated by the mobile station:

   - IMSI detach procedure (with the exceptions specified in section 4.3.4).

ii) MM specific procedures:

A MM specific procedure can only be initiated if no other MM specific procedure is running or no MM connection exists. The procedures belonging to this type are:

- normal location updating procedure;
- periodic updating procedure;
- IMSI attach procedure.

iii) MM connection management procedures:

These procedures are used to establish, maintain and release a MM connection between the mobile station and the network, over which an entity of the upper CM layer can exchange information with its peer. A MM connection establishment can only be performed if no MM specific procedure is running. More than one MM connection may be active at the same time. Depending on how they can be initiated, two types of GMM procedures can be distinguished:

i) GMM common procedures:

Initiated by the network when a GMM context has been established:

- P-TMSI (re-) allocation;
- GPRS authentication and ciphering;
- GPRS identification;
- GPRS information.

ii) GMM specific procedures:

Initiated by the network and used to detach the IMSI in the network for GPRS services and/or non-GPRS services and to release a GMM context:

- GPRS detach.

Initiated by the MS and used to attach or detach the IMSI in the network for GPRS services and/or non-GPRS services and to establish or release a GMM context:

- GPRS attach and combined GPRS attach;
- GPRS detach and combined GPRS detach.

Initiated by the MS when a GMM context has been established:

- normal routing area updating and combined routing area updating;
- periodic routing area updating.

4.1.1.1.1 Integrity Checking of Signalling Messages in the Mobile Station

In UMTS only, integrity protected signalling is mandatory. In UMTS only, all protocols shall use integrity protected signalling. Integrity protection of all layer 3 signalling messages is the responsibility of lower layers. It is the network which activates integrity protection. This is done using the security mode control procedure (TS 25.331).

MM and GMM signalling messages have to be checked for integrity by the MS on a per-message basis. Some MM/GMM messages shall be processed regardless of whether or not integrity protection was activated. Lower layers in the MS provide MM/GMM with an indication for every MM/GMM message as to the result of the integrity checking process:

No integrity check performed;

Integrity check performed and was successful; or

Integrity check performed and was unsuccessful.

Integrity checking on the network side is performed by the RNC and is described in TS 25.413

Not all MM/GMM messages are integrity protected. Therefore, the following MM/GMM messages shall not be discarded by the MM/GMM entity of the MS, regardless of whether they pass or fail the integrity check:

MM messages:

- AUTHENTICATION REQUEST
- AUTHENTICATION FAILURE
- AUTHENTICATION REJECT
- IDENTITY REQUEST
- LOCATION UPDATING REJECT
- CM SERVICE REJECT

GMM messages:

- AUTHENTICATION & CIPHERING REQUEST
- AUTHENTICATION & CIPHERING FAILURE
- AUTHENTICATION & CIPHERING REJECT
- IDENTITY REQUEST
- ATTACH REJECT
- ROUTING AREA UPDATE REJECT
- SERVICE REJECT (UMTS only)

The receiving layer 3 entity in the MS shall not process any other layer 3 signalling messages unless they have been successfully integrity checked by the lower layers. If any signalling messages, having not successfully passed the integrity check, are received by layer 3, the MS shall discard that message.

3GPP TSG-N1/SMG Meeting #10
Abiko, Japan, 11-14 Jan 2000

Document N1-000186
Revision of N1-000043

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	095 r1	Current Version:	3.2.1

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

For submission to:	TSG N #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 13-1-2000

Subject: UMTS security parameters, Combined reject causes for CS and PS

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Reject cause codes for MAC and Synch failure are available for both CS and PS. This CR proposes to use “MAC failure” and “Synch failure” for both PS and CS and use the same code points for these.

Clauses affected: 4.3.2.5.1, 9.2.3a.1,4.7.7.5.1, 9.4.10a.1, 10.5.3.2.2, 10.5.3.6, 10.5.5.14, AnnexG: G.3, G.6

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:

Clarifications and changes since N1-000043

- Offline discussion and confirmation from experts clarifies that if the failure occur at MM auth. then the reject code is directed to the CS domain (MSC) and at GMM auth. failure the reject code is directed to the PS domain (SGSN). The HLR/AuC nodes do not need to know where the failure occurred (i.e. at MM auth. procedure or GMM auth. procedure).
- 10.5.3.2.2: Editorial change
- Cause codes for MAC and Synch failure is changed to No. 20 and 21 in table 10.5.95 and 10.5.147 as well as in Annex G.3.
- Annex G.3: “MSC” is changed to “network”.

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.

9.2.3a.1 Response from SIM

This IE shall be sent if and only if the reject cause was '~~CS s~~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).

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.

9.4.10a.1 Response from SIM

This IE shall be sent if and only if the GMM cause was '~~PS s~~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).

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 s~~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)

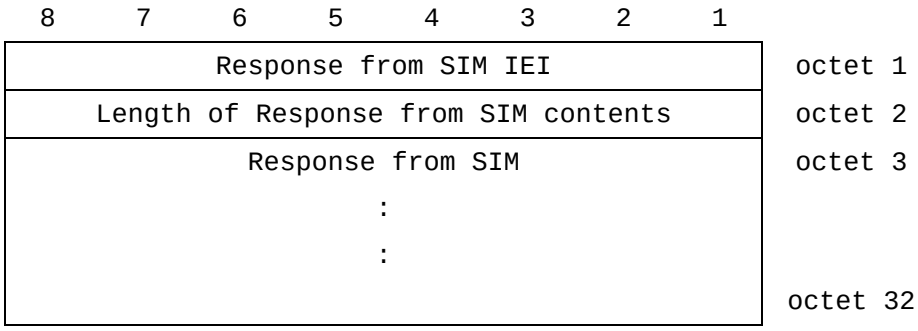

Table 10.5.90.2/TS 24.008: *Response from SIM* information element

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.

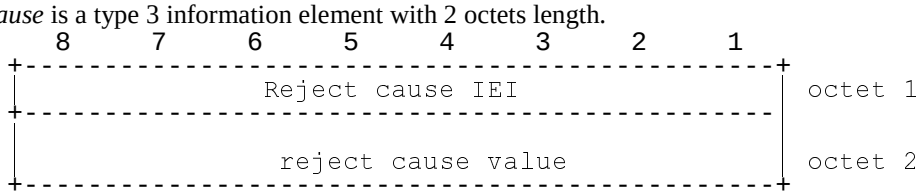

Figure 10.5.81/TS 24.008 *Reject Cause* information element

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 0 0	MAC failure
0 0 0 1 0 1 0 1	Synch 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 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 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.

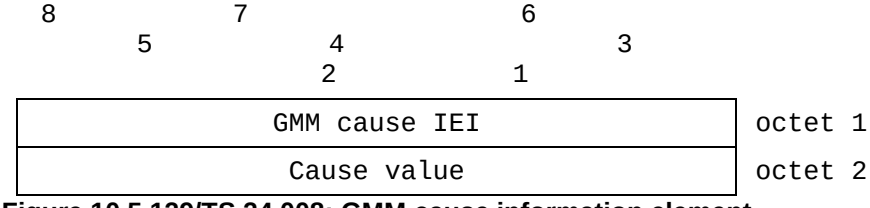

Figure 10.5.129/TS 24.008: GMM cause information element

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 0 0  MAC failure
      0 0 0 1 0 1 0 1  Synch failure
      0 0 0 1 0 1 1 0  Congestion
      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 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

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

Cause value = ~~7 CS~~ 20 MAC failure

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

Cause value = ~~15~~21 ~~CS~~ Synch failure

This cause is sent to the ~~MSC~~ network 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.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)~~

3GPP TSG-N1/SMG Meeting #10
Abiko, Japan, 11-14 Jan 2000

Document N1-000042

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**	**094**	Current Version:	3.2.1

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

For submission to: TSG N #7 *list expected approval meeting # here ↑*

for approval [X] for information [ ]

strategic [ ] non-strategic [ ] *(for SMG 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: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: CN1 **Date:** 22-12-1999

Subject: UMTS security parameters, Correction of format for IE “Response from SIM”

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change: The Information Element “Response from SIM” should be of the format “TLV”.

Clauses affected: 9.4.10a

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:

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	TLV	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).

3GPP TSG-N1/SMG Meeting #10
Abiko, Japan, 11-14 Jan 2000

Document N1-000041

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	093	Current Version:	3.2.1

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

For submission to: TSG N #7 *list expected approval meeting # here ↑*

for approval	X	strategic		*(for SMG use only)*
for information		non-strategic		

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: *(at least one should be marked with an X)*

(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source: CN1 **Date:** 22-12-1999

Subject: UMTS security parameters, Handling of Ciphering algorithm IE in UMTS

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The Ciphering algorithm IE is not used in UMTS. This CR clarifies how an MS shall handle this information.

Clauses affected: 4.7.7.2

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:

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, 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, 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 UMTS, an MS capable of UMTS only shall ignore the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message. An MS capable of both UMTS and GSM shall store the received value in the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message in order to be used at an inter system change from UMTS to GSM.

In GSM, if the AUTHENTICATION AND CIPHERING REQUEST message does not include either the GPRS or the UMTS authentication parameters (RAND and GPRS CKSN or 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, 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]).