3GPP TSG_CN **Tdoc NP-000273**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source: **TSG_N WG “1”**

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

Agenda item: **6.3**

Document for: **APPROVAL**

Introduction:

This document contains **“6”** CRs on **Work Item “Security”,** that have been agreed by **TSG_N WG “1”,** and are forwarded to **TSG_N Plenary** meeting #8 for approval.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N1-000747	24.011	CR006	1	C	R99	3.2.0	3.3.0	Alignment of SMS protocol with current MM/GMM integrity protection rules
N1-000663	24.008	CR137	1	C	R99	3.3.1	3.4.0	Network Authentication Failure
N1-000744	24.008	CR207	1	F	R99	3.3.1	3.4.0	Integrity checking of MM/GMM messages and integrity protection during emergency call
N1-000745	24.008	CR213	1	C	R99	3.3.1	3.4.0	Alignment of CC and SM protocols with current MM/GMM integrity protection rules
N1-000785	24.008	CR216	2	F	R99	3.3.1	3.4.0	Correction of the MM Authentication procedure
N1-000749	24.008	CR217		F	R99	3.3.1	3.4.0	Correction of the GMM Authentication and ciphering procedure

3GPP/SMG Meeting #12
Oahu/Hawaii, USA, 22 May - 26 May.2000

Document N1-000663
Revised from
N1-000314

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**	**137r1**	Current Version:	3.3.1

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

For submission to:	CN #7	for approval	☒	strategic	□
list expected approval meeting # here ↑		for information	□	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: (U)SIM □　ME ☒　UTRAN / Radio □　Core Network ☒
(at least one should be marked with an X)

Source: Vodafone AirTouch Plc　　**Date:** 18/05/2000

Subject: MS behaviour when detecting a 'bad' network from an authentication challenge

Work item: Security

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

Reason for change:

There is currently no procedure defined for how the MS should react upon receipt of an invalid Message Authentication Code (MAC) which is derived from the AUTN provided in the UMTS authentication challenge.

The MAC provides a guarantee of 'freshness' for the authentication challenge. For instance, in GSM, a RAND could be captured and replayed later without the MS knowing that the RAND had been intercepted. In UMTS, the MS can tell that the RAND is not fresh.

This CR proposes a suitable procedure:

- Upon sending the AUTHENTICATION FAILURE or the AUTHENTICATION & CIPHERING FAILURE message the MS starts a timer.
- Upon expiry of the timer the MS deems the network to be false.
- Upon receipt of a failure message with reject cause 'MAC failure' the network may send an IDENTITY REQUEST message. Upon receipt of the IDENTITY REQUEST message, the MS shall stop the timer and send its (encrypted) IMSI to the network in the IDENTITY RESPONSE message. A second timer shall be started.
- Having sent the IDENTITY RESPONSE message, the MS may then receive a new authentication challenge. If it does then it shall stop the second timer. If the new challenge contains an invalid MAC then the MS shall deem the network as being false. If no new authentication challenge is received, the second timer will expire and the MS shall deem the network as being false.
- Once the MS has deemed the network to be false, an internal mechanism shall treat the cell (as identified by the BSIC, ARFCN and timing) as barred and shall prevent the MS from camping on that cell, until a refresh of System Information data.

Clauses affected: 4.3.2.5.1, 4.3.2.6, 4.3.2.6.1, 4.7.7.5.1, 4.7.7.6, 4.7.7.6.1, 11.2, 11.2.2

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 GSM 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 an AUTHENTICATION FAILURE message to the network, with the ~~failure~~reject cause ‘MAC failure’~~ (see 33.102)~~. The MS shall then follow the procedure described in section 4.3.2.6 (c).

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 AUTHENTICATION FAILURE message to the network, with the ~~failure~~reject cause ‘Synch failure’ and parameters provided by the SIM (see TS 33.102) The MS shall then follow the procedure described in section 4.3.2.6 (d).

~~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.

(c) Authentication failure (reject cause ‘MAC failure’):

The MS shall send an AUTHENTICATION FAILURE message, with reject cause ‘MAC failure’, to the network and start timer T3214. Upon receipt of an AUTHENTICATION FAILURE message from the MS, with reject cause ‘MAC failure,’ the network may initiate the identification procedure described in section 4.3.3. This is to allow the network to obtain the IMSI from the MS. The network may then check that the TMSI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the MS shall stop timer T3214 if running and then send the IDENTITY RESPONSE message. At the sending of this message, the MS shall start the timer T3215.

If the TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the MS. Upon receiving the second AUTHENTICATION REQUEST message from the network, the MS shall stop the timer T3215, if running, and then process the challenge information as normal.

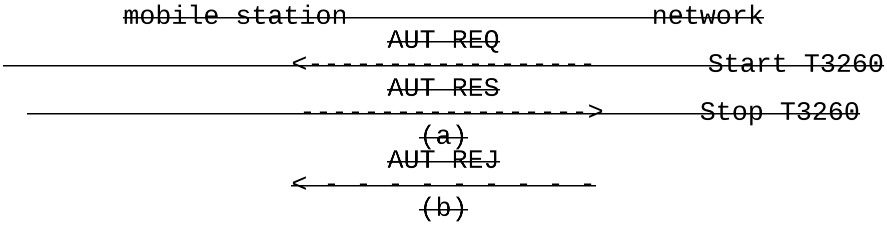
When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).

Upon successfully validating the network (an AUTHENTICATION REQUEST containg a valid MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall resume any retransmission timers (e.g. T3210, T3220 or T3230) that are currently suspended if they are not not already running.

It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occur:

- After sending the AUTHENTICATION FAILURE message with the reject cause ‘MAC failure’ the timer T3214 times out;
- After sending the IDENTITY RESPONSE message the timer T3215 times out; or
- Upon receipt of the second AUTHENTICATION REQUEST, the MAC value still cannot be resolved.

When it has been deemed by the MS that the source of the authentication challenge is not genuine (authentication not accepted by the MS), the MS shall behave as described in section 4.3.2.6.1



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

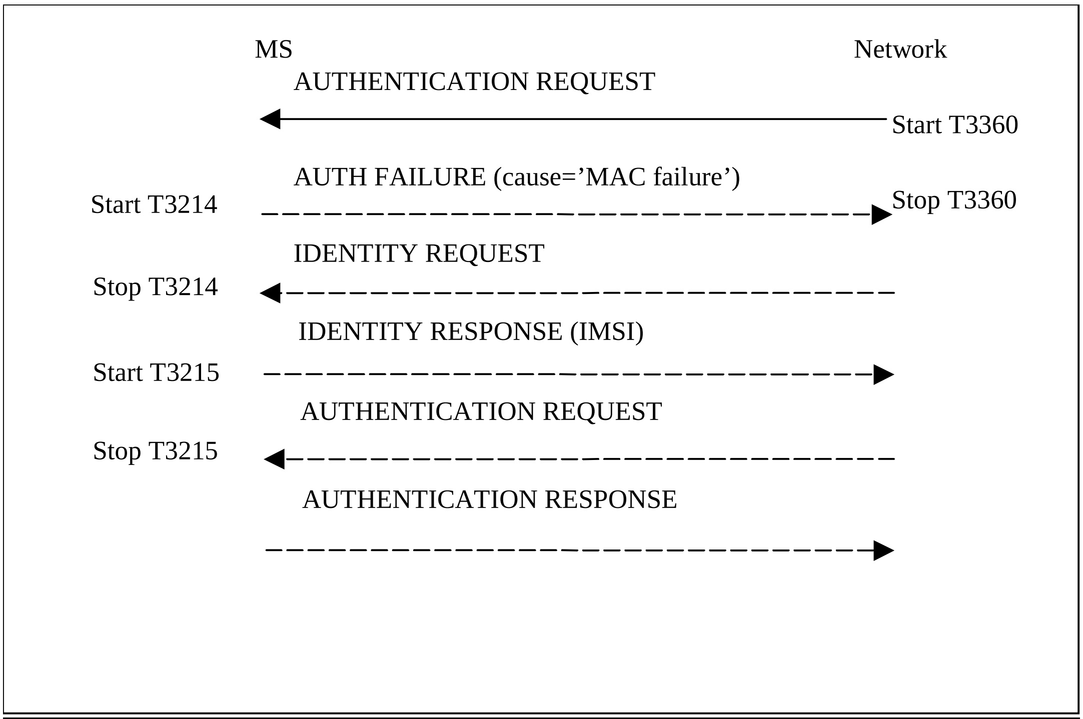


Figure 4.2/TS 24.008: Authentication Failure Procedure (reject cause ‘MAC failure’)

(d) Authentication failure (reject cause ‘synch failure’):

The MS shall send an AUTHENTICATION FAILURE message, with reject cause ‘synch failure,’ to the network and start the timer T3216. Upon receipt of an AUTHENTICATION FAILURE message from the MS with the reject cause ‘synch failure,’ the network shall use the returned AUTS parameter from the authentication failure parameter IE in the AUTHENTICATION FAILURE message, to re-synchronise. The re-synchronisation procedure requires the VLR/MSC to delete all unused authentication vectors for that IMSI and obtain new vectors from the HLR. When re-synchronisation is complete, the network shall initiate the authentication procedure. Upon receipt of the AUTHENTICATION REQUEST message, the MS shall stop the timer T3216, if running. If the timer T3216 times out, the MS shall behave as described in section 4.3.2.6.1

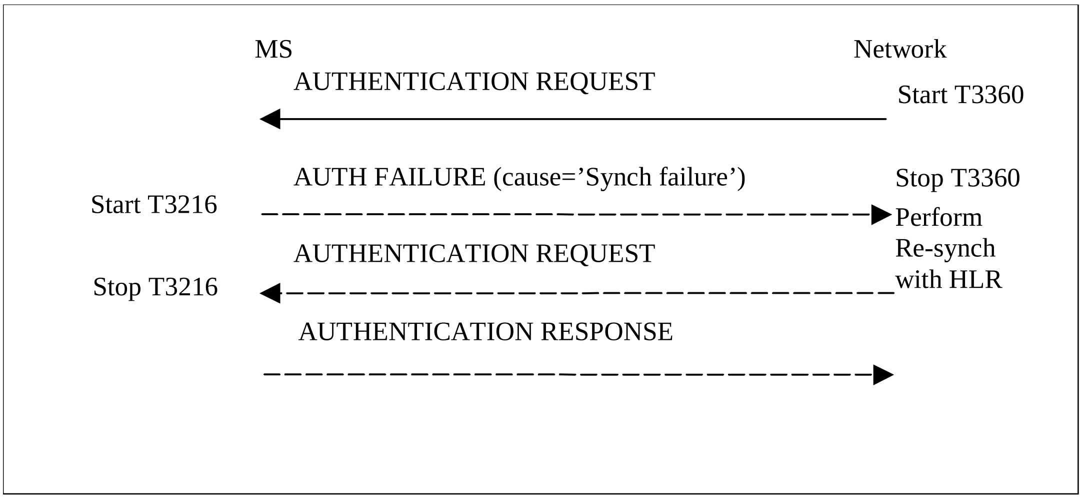


Figure 4.2/TS 24.008: Authentication Failure Procedure (reject cause ‘MAC failure’)

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then the it shall treat the current serving cell where the authentication failure occurred as barred, until refresh of system information data

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

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 AUTHENTICATION AND CIPHERING FAILURE message to the network, with the ~~failure~~GMM cause ‘MAC failure’~~ and parameters provided by the SIM (see TS 33.102)~~. The MS shall then follow the procedure described in section 4.7.7.6 (f).

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 AUTHENTICATION AND CIPHERING FAILURE message to the network, with the ~~failure~~GMM cause ‘Synch failure’ and parameters provided by the SIM (see TS 33.102). The MS shall then follow the procedure described in section 4.7.7.6 (g).

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

4.7.7.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

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

b) Expiry of timer T3360

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

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

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

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

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

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

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

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

GPRS detach containing cause "power off":

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

GPRS detach containing other causes than "power off":

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

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

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

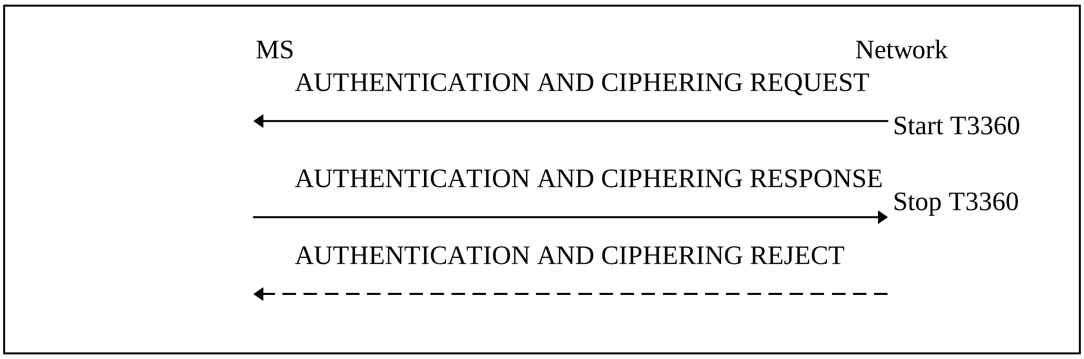

MS
Network
AUTHENTICATION AND CIPHERING REQUEST
Start T3360
AUTHENTICATION AND CIPHERING RESPONSE
Stop T3360
AUTHENTICATION AND CIPHERING REJECT

Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

(f) Authentication failure (GMM cause ‘MAC failure’)

The MS shall send an AUTHENTICATION & CIPHERING FAILURE message, with GMM cause ‘MAC failure’ to the network and start timer T3318. Upon receipt of an AUTHENTICATION & CIPHERING FAILURE message from the MS with GMM cause ‘MAC failure’ the network may initiate the identification procedure described in section 4.7.8. This is to allow the network to obtain the IMSI from the MS. The network may then check that the P-TMSI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the MS shall stop timer T3318, if running, and then send the IDENTITY RESPONSE message. At the sending of this message, the MS shall start the timer T3319.

If the P-TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION & CIPHERING REQUEST message to the MS. Upon receiving the second AUTHENTICATION & CIPHERING REQUEST message from the network, the MS shall stop timer T3319, if running, and then process the challenge information as normal.

When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

Upon successfully validating the network, (an AUTHENTICATION & CIPHERING REQUEST message containing a valid MAC is received), the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall resume any retransmission timers (i.e. T3310, T3321, T3330 or T3317) that are currently suspended, if they are not already running.

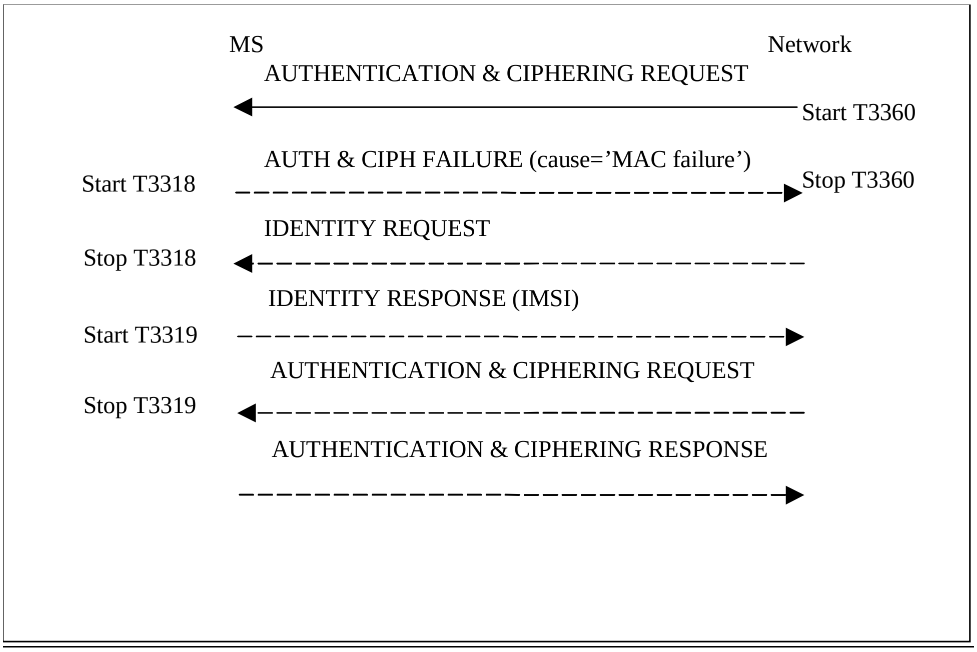
It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occur:

- After sending the AUTHENTICATION & CIPHERING FAILURE message with GMM cause ‘MAC failure’ the timer T3318 times out;

- After sending the IDENTITY RESPONSE message to the network, the timer T3319 times out; or

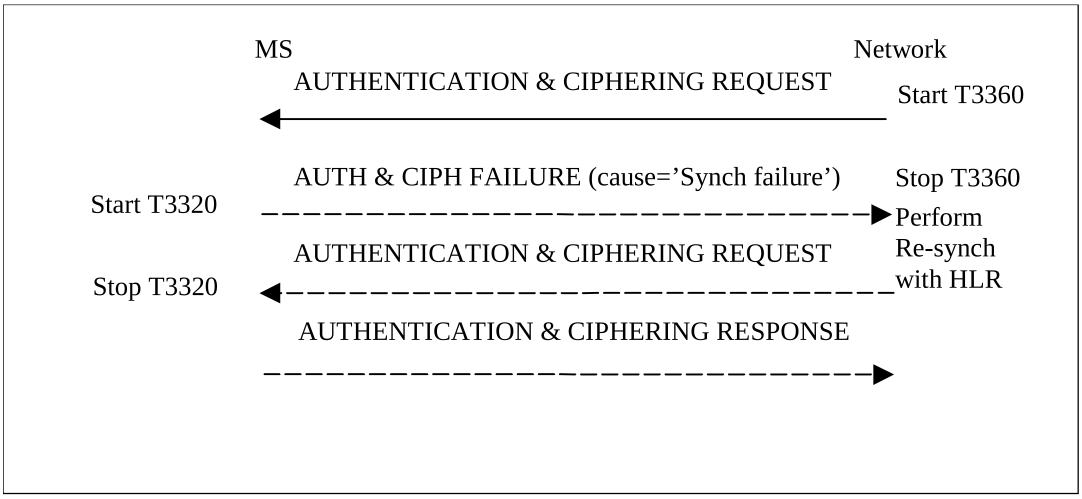
- Upon receipt of the second AUTHENTICATION & CIPHERING REQUEST message from the network, the MAC value still cannot be resolved.

When it has been deemed by the MS that the source of the authentication challenge is not genuine (authentication not accepted by the MS), the MS shall behave as described in section 4.7.7.6.1.


MS
Network
AUTHENTICATION & CIPHERING REQUEST
Start T3360
AUTH & CIPH FAILURE (cause=’MAC failure’)
Start T3318
Stop T3360
IDENTITY REQUEST
Stop T3318
IDENTITY RESPONSE (IMSI)
Start T3319
AUTHENTICATION & CIPHERING REQUEST
Stop T3319
AUTHENTICATION & CIPHERING RESPONSE

(g) Authentication failure (GMM cause ‘Synch failure’):

The MS shall send an AUTHENTICATION & CIPHERING FAILURE message, with the GMM cause 'Synch failure,' to the network and start the timer T3320. Upon receipt of an AUTHENTICATION & CIPHERING message from the MS with the GMM cause 'synch failure,' the network shall use the returned AUTS parameter from the authentication & ciphering failure parameter IE in the AUTHENTICATION & CIPHERING FAILURE message, to re-synchronise. The re-synchronisation procedure requires the SGSN to delete all unused authentication vectors for that IMSI and obtain new vectors from the HLR. When re-synchronisation is complete, the network shall initiate the authentication & ciphering procedure. Upon receipt of the AUTHENTICATION & CIPHERING REQUEST message, the MS shall stop timer T3320, if running. If the timer T3320 times out, the MS shall behave as described in section 4.7.7.6.1.


MS
Network
AUTHENTICATION & CIPHERING REQUEST
Start T3360
AUTH & CIPH FAILURE (cause='Synch failure')
Stop T3360
Start T3320
Perform
Re-synch
with HLR
AUTHENTICATION & CIPHERING REQUEST
Stop T3320
AUTHENTICATION & CIPHERING RESPONSE

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then it shall treat the current serving cell where the authentication failure occurred as barred, until refresh of system information data.

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

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 up dating fai lure	- expiry - change of BCCH parameter	new random attempt
T3214	3 5 7	5s	-AUTHENT FAILURE-cause=MAC failure sent	- ID REQUEST - received	Consider the network as 'false'(see 4.3.2.6.1)
T3215	3 5 7	15s	-ID RESPONSE sent	-AUTHENT REQ -received	Consider the network as 'false' (see 4.3.2.6.1)
T3216	3 5 7	15s	-AUTHENT FAILURE-cause=synch failure sent	-AUTHENT REQ -received	Consider the network as 'false' (see 4.3.2.6.1)
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 STAT	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 connection	
T3255		Note	LOC UPD ACC sent with "Follow on Proceed"	CM SERVICE REQUEST	Release RR Connection or use for mobile station terminating call	
T3260	5	12s	AUTHENT-REQUEST sent	AUTHENT-RESPONSE received AUTHENT-FAILURE received	Optionally Release RR connection Procedural behavior is FFS	
T3270	4	12s	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Optionally Release RR connection	

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

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

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 1^{st} , 2^{nd}, 3^{rd} , 4^{th} 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
T3318	5s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=MAC failure) sent	IDENTITY REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
T3319	15s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	IDENTITY RESPONSE sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
T3320	15s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=synch failure) sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
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	Default 12 min Note 1	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
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.

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

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1^{st}, 2^{nd}, 3^{rd}, 4^{th} 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
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 Meeting #12
Hawaii, USA, 22-26 May 2000

Document N1-000744
Revision of N1-000647

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**	**207r1**	Current Version:	3.3.1

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

For submission to:	CN #8	for approval	X	Strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*use only)*

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

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

Source:	Ericsson, Vodafone	**Date:**	2000-05-15

Subject: Integrity checking of MM/GMM messages and integrity protection during emergency calls

Work item: Security

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

Reason for change:

The supervision on that integrity protection is activated is the responsibility of the MM and GMM layer in the MS according to TS 33.102. In order to do this, the lower layers has to send an indication to the MM/GMM layer when integrity protection is started for that domain.

For the establishment of a MM connection for an emergency call when no other MM connection is established, the core network is not required to initiate a security mode control procedure for the CS domain in order to activate integrity protection. For the establishment of a MM connection for an emergency call when no other MM connections are established, the MM layer in the MS shall not supervise whether integrity protection is activated or not in the MS.

Furthermore this CR proposes to add the following MM and GMM messages to the list of MM/GMM messages which the MS is allowed to handle if they are received before the integrity protection is activated in the MS (for respectively CN domain):

- LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
- ABORT - The abort procedure may be invoked by the network to abort any on-going MM connection establishment
- ROUTING AREA UPDATE ACCEPT (at periodic routing area update with no change of routing area or temporary identity)

In this revision of the CR, the DETACH ACCEPT has been added to the list of GMM messages that CAN be received by the GMM entity in the MS prior to receipt of the indication that integrity protection has started. The reason for this addition is that the DETACH REQUEST (at non power-off) message does not contain the CKSN IE and so the network can not trigger the security mode control procedure. The DETACH REQUEST (at non power-off) message can be an initial layer three message and so if no security mode control procedure can be performed, then the network has to send the DETACH ACCEPT as a non-integrity protected message. There is no security risk, because the MS only accepts the DETACH ACCEPT message if it has sent a request.

Clauses affected:	4.1.1.1.1, 4.1.1.1.1a, 4.5.1.1

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:	In Annex A, chapters 6.4.5 “Security mode set-up procedure” and 6.5.1 “Access link data integrity – general” from TS 33.102 (Stage 2 of 3G Security) are attached.

4.1.1.1.1 Integrity Checking of Signalling Messages in the Mobile Station (UMTS only)

In UMTS only, integrity protected signalling is mandatory with one exception regarding emergency calls (see 4.1.1.1.1a). In UMTS only, all layer 3 protocols shall use integrity protected signalling once the security mode procedure has been successfully activated in the network and the MS. 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).

The supervision that integrity protection is activated shall be the responsibility of the MM and GMM layer in the MS (see TS 33.102). In order to do this, the lower layers shall provide the MM and GMM layer with an indication on when the integrity protection is activated in the MS (i.e. one indication to the MM layer when a security mode control procedure for the CS domain is processed successfully and one indication to the GMM layer when a security mode control procedure for the PS domain is processed successfully).

The CS and PS domains in the network and the MM and GMM layers in the MS, are not aware of whether integrity protection has been started in the lower layers by the other domain.

~~NOTE:~~ It is mandatory for the network to initiate one security mode control procedure for the CS domain and one for the PS domain.

~~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~~accepted by the MM~~/~~ and GMM entit~~y~~ies of the MS if they are received, before the security mode control procedure for that domain is activated in the lower layers in the MS~~, regardless of whether they pass or fail the integrity check~~:

- MM messages:
    - AUTHENTICATION REQUEST
    - AUTHENTICATION REJECT
    - IDENTITY REQUEST
    - LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
    - LOCATION UPDATING REJECT
    - CM SERVICE REJECT
    - ABORT
- GMM messages:
    - AUTHENTICATION & CIPHERING REQUEST
    - AUTHENTICATION & CIPHERING REJECT
    - IDENTITY REQUEST
    - ATTACH REJECT
    - ROUTING AREA UPDATE ACCEPT (at periodic rouoting area update with no change of routing area or temporary identity)

- ROUTING AREA UPDATE REJECT
- SERVICE REJECT ~~(UMTS only)~~
- DETACH ACCEPT (for non power-off)

No other MM/GMM signalling messages shall be processed by the receiving MM and GMM entities unless the security mode control procedure is activated for that domain. Furthermore, the receiving MM and GMM entities in the MS shall not forward any CM layer messages to the CM sub-layer unless the security mode control procedure is activated for that domain.

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 once integrity protection is activated. If any signalling messages, having not successfully passed the integrity check, are received ~~by layer 3~~, then the lower layers in the MS shall discard that message (see TS 25.331). If any layer 3 signalling message is received, in either PS or CS domains, as not integrity protected even though the integrity protection has been activated in the MS by that~~either the PS or CS~~ domain in the network, then the lower layers shall discard this message (see TS 25.331).

Integrity checking on the network side is performed by the RNC and is described in TS 25.331.

4.1.1.1.1a Integrity protection for emergency call (UMTS only)

For the establishment of a MM connection for an emergency call when no other MM connection is established (e.g. for an emergency call initiated without a SIM no other MM connections can exist), the core network ~~is~~need not ~~required to~~ initiate a security mode control procedure for the CS domain in order to activate integrity protection.

~~-~~For the establishment of a MM connection for an emergency call when no other MM connections are established, the MM layer in the MS shall not supervise whether integrity protection is activated or not in the MS.

For the establishment of a MM connection for an emergency call when one or more MM connections are already established, the integrity protection is already activated by the network.

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

4.5.1 MM connection establishment

4.5.1.1 MM connection establishment initiated by the mobile station

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

- An MM connection establishment may only be initiated by the mobile station when the following conditions are fulfilled:
    - Its update status is UPDATED.
    - The MM sublayer is in one of the states MM IDLE or MM connection active but not in MM connection active (Group call).

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

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

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

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

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

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

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

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

c) Only applicable for mobile stations supporting VGCS talking:

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

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

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

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

The CM SERVICE REQUEST message contains the

- mobile identity according to section 10.5.1.4;

- mobile station classmark 2;

- ciphering key sequence number; and

- CM service type identifying the requested type of transaction (e.g. mobile originating call establishment, emergency call establishment, short message service, supplementary service activation, location services)

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

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

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

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

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

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

In GSM, the network decides also if the ~~security~~ciphering mode setting procedure shall be invoked (see section 3.4.7 in GSM 04.18)..

In UMTS, the network decides also if the security mode control procedure shall be invoked (see section 8.1.10 in TS 25.331).

NOTE: If the CM_SERVICE_REQUEST message contains a priority level the network may use this to perform queuing and pre-emption as defined in TS 23.067.

In GSM, an indication from the RR sublayer that the ~~security~~ciphering mode setting procedure is completed, or reception of a CM SERVICE ACCEPT message, shall be treated as a service acceptance indication by the mobile station.

In UMTS, an indication from the RR sublayer that the security mode control procedure is completed, or reception of a CM SERVICE ACCEPT message, shall be treated as a service acceptance indication by the mobile station. The procedures in section 4.1.1.1.1 shall always have precedence over this section.

In UMTS, during a MM connection establishment for all services, except for emergency call when no other MM connection exists (see chapter 4.1.1.1.1a), the security mode control procedure with activation of integrity protection shall be invoked by the network unless integrity protection is already started (see chapter 4.1.1.1.1).

The MM connection establishment is completed, timer T3230 shall be stopped, the CM entity that requested the MM connection shall be informed, and MM sublayer state MM CONNECTION ACTIVE is entered. The MM connection is considered to be active.

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

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

#4 :	IMSI unknown in VLR
#6 :	Illegal ME
#17 :	Network failure
#22 :	Congestion
#32 :	Service option not supported
#33 :	Requested service option not subscribed
#34 :	Service option temporarily out of order

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

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

- If the cause value is not #4 or #6 the MM sublayer returns to the previous state (the state where the request was received). Other MM connections shall not be affected by the CM SERVICE REJECT message.
- If cause value #4 is received, the mobile station aborts any MM connection, deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to NOT UPDATED (and stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. If subsequently the RR connection is released or aborted, this will force the mobile station to initiate a normal location updating). Whether the CM request shall be memorized during the location updating procedure, is a choice of implementation.
- If cause value #6 is received, the mobile station aborts any MM connection, deletes any TMSI, LAI and ciphering key sequence number in the SIM, changes the update status to ROAMING NOT ALLOWED (and

stores it in the SIM according to section 4.1.2.2), and enters the MM sublayer state WAIT FOR NETWORK COMMAND. The mobile station shall consider the SIM as invalid until switch-off or the SIM is removed.

*** Annex A, chapter 6.4.5 and 6.5.1 from TS 33.102 ver. 3.4.0 ***

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- **If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.**
- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

6.5 Access link data integrity

6.5.1 General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the UE and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. **The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).**

All signalling messages except the following ones shall then be integrity protected:

- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- System Information (broadcasted information).

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

Document N1-000745
Revised from N1-000664

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 213r1 Current Version: 3.3.1

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

For submission to: CN #8
list expected approval meeting # here ↑

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

Source: Vodafone AirTouch, Ericsson **Date:** 15th May 2000

Subject: Alignment of CC and SM protocols with current MM/GMM integrity protection rules

Work item: Security

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

F	Correction	□	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	☒
			Release 00	□

Release:

Reason for change: In UMTS, all signalling messages for all protocols shall be integrity protected. This CR adds that requirement to the CC and SM protocol descriptions.

Clauses affected: 5, 6.1

Other specs affected:

Other 3G core specifications	☒	→ List of CRs:	24.010 – N1-000746 24.011 – N1-000747
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.

5 Elementary procedures for circuit-switched Call Control

5.1 Overview

5.1.1 General

This section describes the call control (CC) protocol, which is one of the protocols of the Connection Management (CM) sublayer (see TS 24.007).

Every mobile station must support the call control protocol. If a mobile station does not support any bearer capability at all then it shall respond to a SETUP message with a RELEASE COMPLETE message as specified in section 5.2.2.2.

In UMTS only, integrity protected signalling (see section 4.1.1.1.1 of this specification and in general, see TS 33.102) is mandatory. In UMTS only, all protocols shall use integrity protected signalling. Integrity protection of all CC~~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).

In the call control protocol, more than one CC entity are defined. Each CC entity is independent from each other and shall communicate with the correspondent peer entity using its own MM connection. Different CC entities use different transaction identifiers.

With a few exceptions this Technical Specification describes the call control protocol only with regard to two peer entities. The call control entities are described as communicating finite state machines which exchange messages across the radio interface and communicate internally with other protocol (sub)layers. This description is only normative as far as the consequential externally observable behaviour is concerned.

Certain sequences of actions of the two peer entities compose "elementary procedures" which are used as a basis for the description in this section. These elementary procedures may be grouped into the following classes:

- call establishment procedures;
- call clearing procedures;
- call information phase procedures;
- miscellaneous procedures.

The terms "mobile originating" or "mobile originated" (MO) are used to describe a call initiated by the mobile station. The terms "mobile terminating" or "mobile terminated" (MT) are used to describe a call initiated by the network.

Figure 5.1a/TS 24.008 gives an overview of the main states and transitions on the mobile station side.

The MS side extension figure 5.1a.1/TS 24.008 shows how for the Network Initiated MO call the MS reaches state U1.0 from state U0 $(CCBS)$.

Figure 5.1b/TS 24.008 gives an overview of the main states and transitions on the network side.

The Network side extension figure 5.1b.1/TS 24.008 shows for Network Initiated MO Calls the Network reaches state N1.0 from state N0 $(CCBS)$.

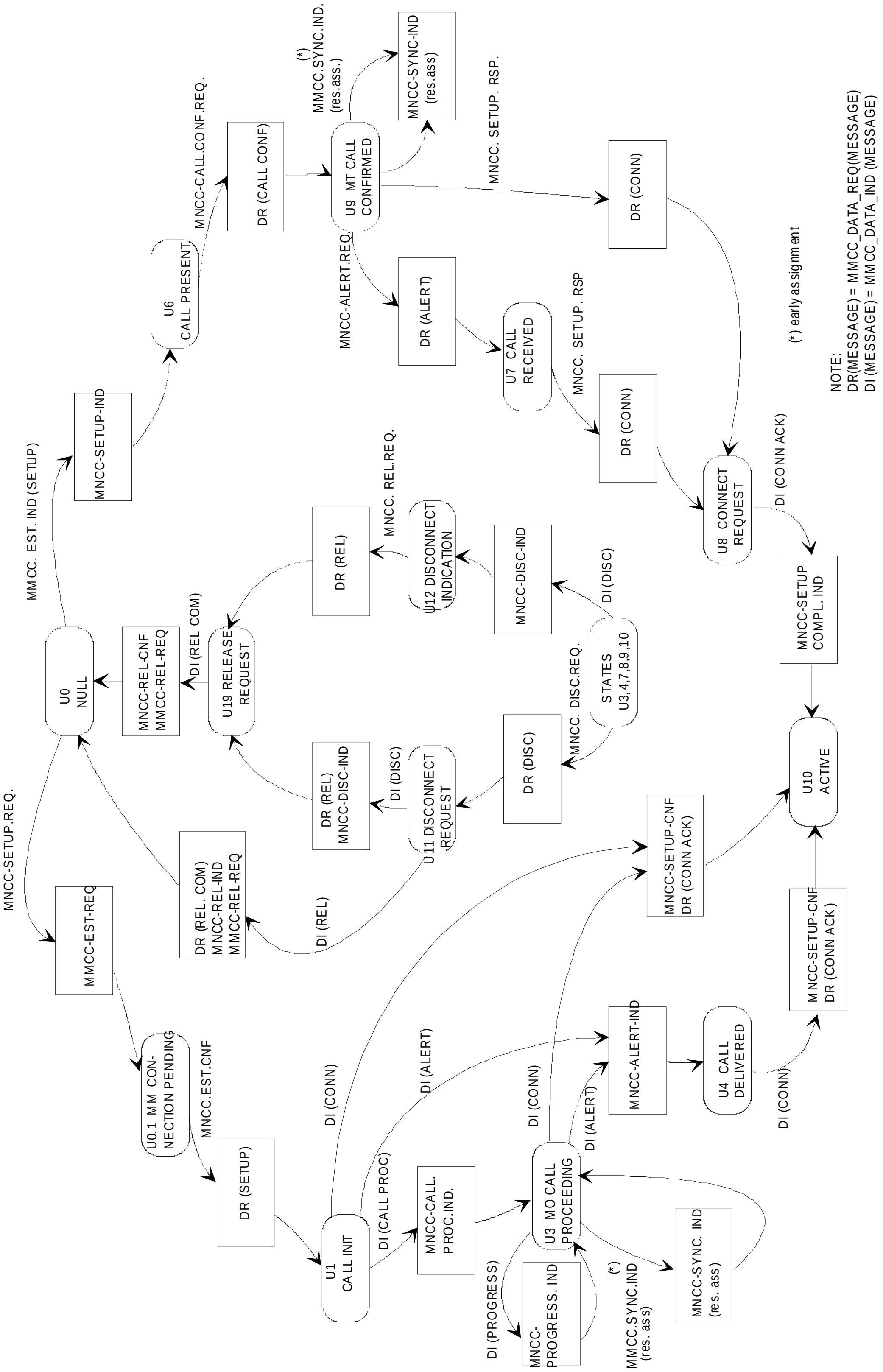


Figure 5.1a/TS 24.008
Overview call control protocol/MS side

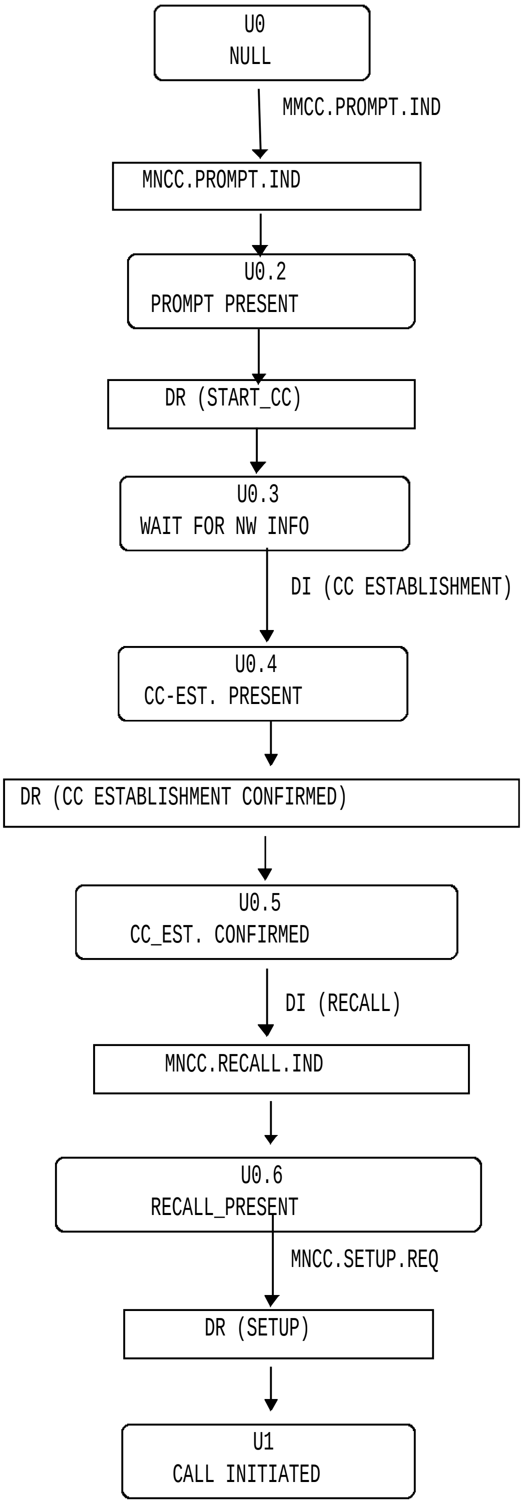


Figure5.1a.1/TS 24.008
Overview call control protocol/MS side, extension:

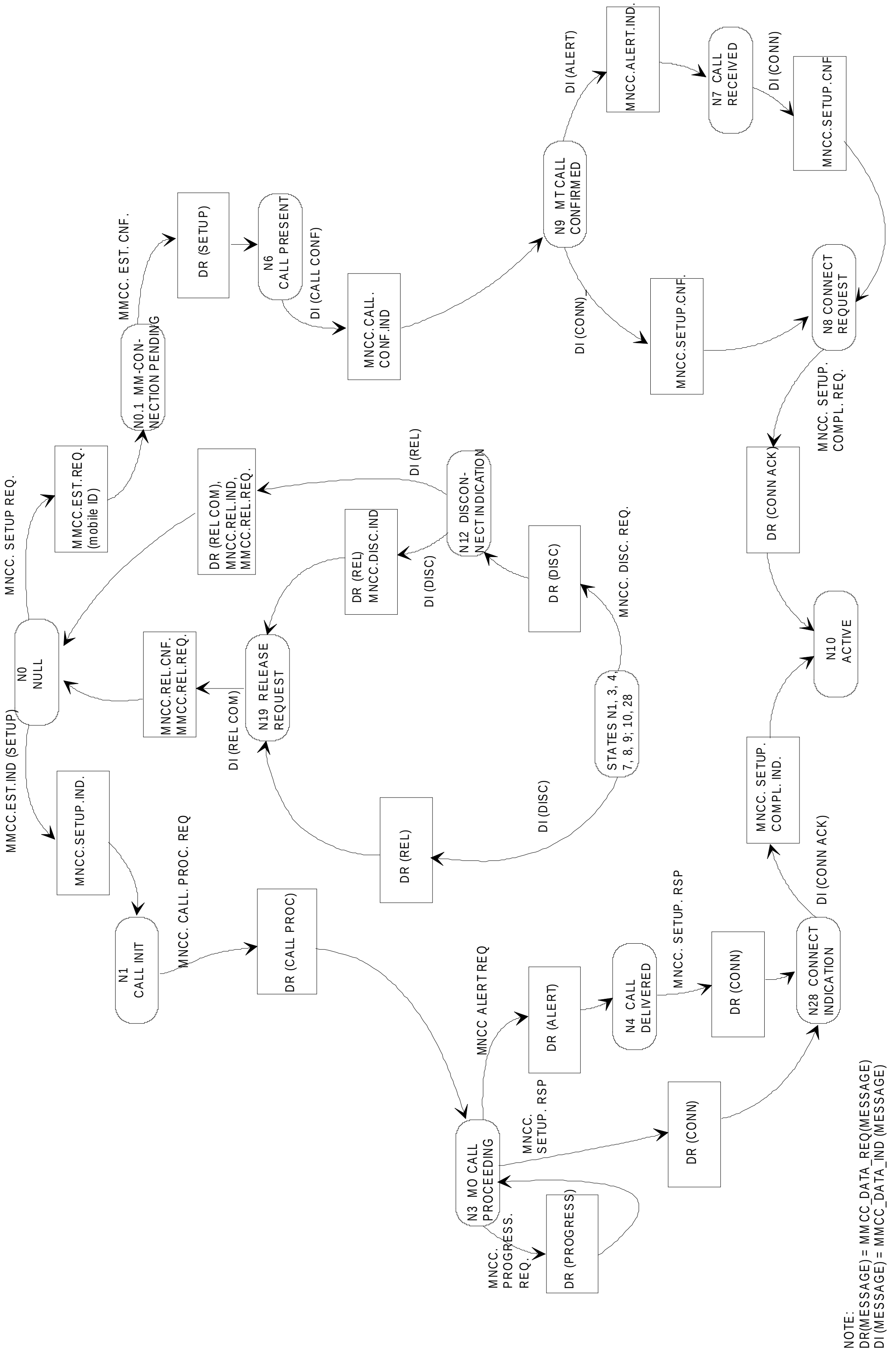


Figure 5.1b/TS 24.008 Overview call control protocol/Network side

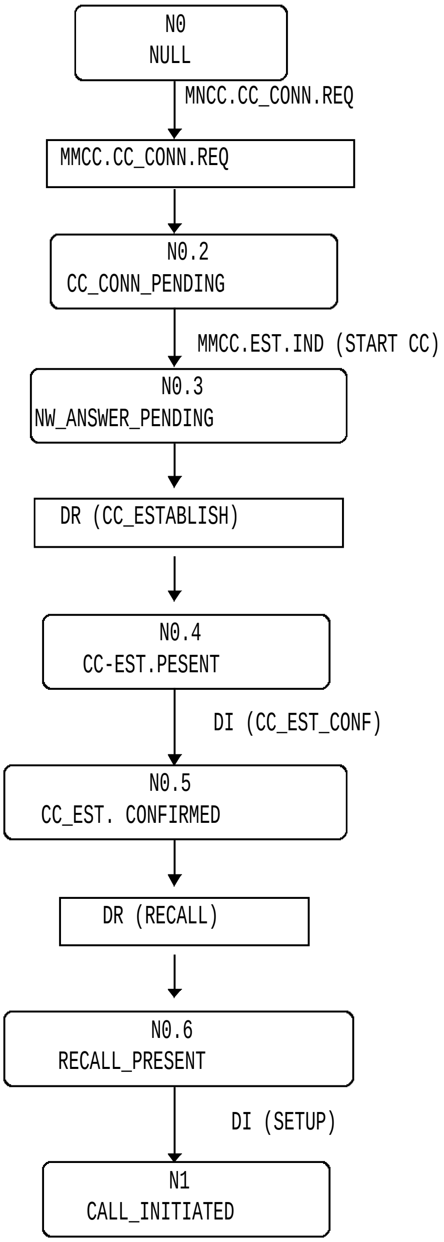


Figure 5.1b.1/TS 24.008 Overview call control protocol/Network side, extension

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

6.1 GPRS Session management

6.1.1 General

The main function of the session management (SM) is to support PDP context handling of the user terminal. The SM comprises procedures for

identified PDP context activation, deactivation and modification; SM procedures for identified access can only be performed if a GMM context has been established between the MS and the network. If no GMM context has been established, the MM sublayer has to initiate the establishment of a GMM context by use of the GMM procedures as described in chapter 4. After GMM context establishment, SM uses services offered by GMM (see TS 24.007 [20]). Ongoing SM procedures are suspended during GMM procedure execution.

In UMTS only, integrity protected signalling (see section 4.1.1.1.1 of this specification and in general, see TS 33.102) is mandatory. In UMTS only, all protocols shall use integrity protected signalling. Integrity protection of all SM~~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).

For the session management protocol, the extended TI mechanism may be used (see 24.007).

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

Document N1-000747
Revision of N1-000666

CHANGE REQUEST

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

24.011 CR 006r1 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 #8
list expected approval meeting # here ↑

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

Source: Vodafone AirTouch, Ericsson **Date:** 15th May 2000

Subject: Alignment of SMS protocol with current MM/GMM integrity protection rules

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	☒	
D	Editorial modification	□	

Release:

Phase 2	□
Release 96	□
Release 97	□
Release 98	□
Release 99	☒
Release 00	□

Reason for change: In UMTS, all signalling messages for all protocols shall be integrity protected. This CR adds that requirement to the SMS protocol description.

Clauses affected: 2.1

Other specs affected:

Other 3G core specifications	☒	→ List of CRs:	24.008 – N1-000745 24.010 – N1-000746
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.

2.1 Protocols and protocol architecture

In UMTS only, integrity protected signalling (see ~~section 4.1.1.1.1 of~~ TS 24.008, subclause ‘Integrity Protection of Signalling Messages,’ and in general, see TS 33.102) is mandatory. In UMTS only, all protocols shall use integrity protected signalling. Integrity protection of all SMS~~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).

The hierarchical model in Figure 2.1a shows the layer structure of the MSC and the MS in GSM. The hierarchical model in Figure 2.1c shows the layer structure of the SGSN and the MS in UMTS.

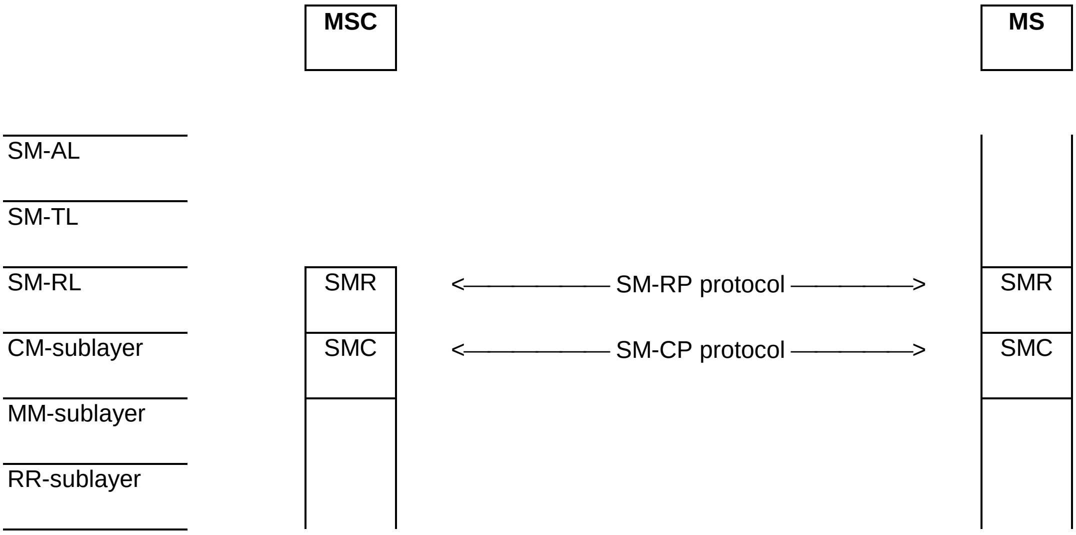


Figure 2.1a/TS 24.011: Protocol hierarchy for circuit switched service

The hierarchical model in Figure 2.1b shows the layer structure of the SGSN and the MS.

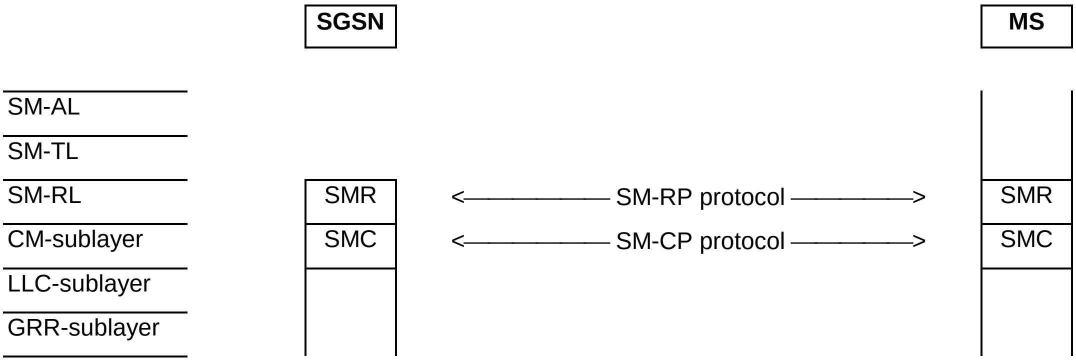


Figure 2.1b/TS 24.011: Protocol hierarchy for GPRS in GSM

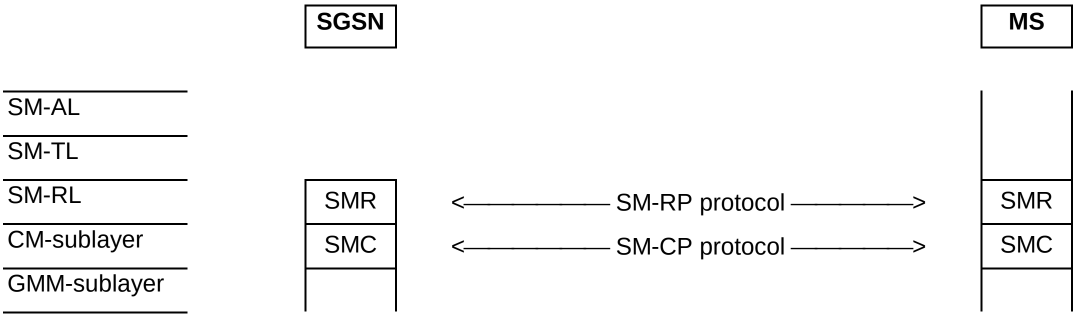


Figure 2.1c/24.011: Protocol hierarchy for packet switched service in UMTS

The CM-sublayer, in terms of the Short Message Service Support, provides services to the Short Message Relay Layer.

On the MS-side the Short Message Relay Layer provides services to the Short Message Transfer Layer. The Short Message Relay Layer is the upper layer on the network side (MSC or SGSN), and the SM-user information elements are mapped to TCAP/MAP.

The peer protocol between two SMC entities is denoted SM-CP, and between two SMR entities, SM-RP.

Abbreviations:

SM-AL	Short Message Application Layer
SM-TL	Short Message Transfer Layer
SM-RL	Short Message Relay Layer
SM-RP	Short Message Relay Protocol
SMR	Short Message Relay (entity)
CM-sub	Connection Management sublayer
SM-CP	Short Message Control Protocol
SMC	Short Message Control (entity)
MM-sub:	Mobility Management sublayerGMM-sub: GPRS Mobility Management sublayer
RR-sub:	Radio Resource Management sublayer
LLC-sub	Logical Link Control sublayer
GRR-sub	GPRS Radio Resource sublayer in GSM

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

Document ***N1-000749***
revision of N1-000672
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**	**217r1**	Current Version:	3.3.1

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

For submission to:	CN#8	for approval	☒	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	☒	UTRAN / Radio	□	Core Network	☒

Source:	Siemens AG	**Date:**	24.05.2000

Subject: Correction of the GMM Authentication and ciphering procedure

Work item: Security

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

Reason for change: The length of various authentication parameters was changed by CR 33.102-37r1.

Clauses affected: 4.7.7, 9.4.9, 9.4.10

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.

4.7.7 Authentication and ciphering procedure

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

The purpose of the authentication and ciphering procedure is fourfold (see TS 33.102):

- to permit the network to check whether the identity provided by the MS is acceptable or not~~, see TS 33.102)~~;
- to provide parameters enabling the MS to calculate a new GPRS UMTS ciphering key and a new GPRS UMTS integrity key.
- to let the network set the GSM ciphering mode (ciphering /no ciphering) and GSM ciphering algorithm; and
- to permit the mobile station to authenticate the network.

In 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 TS 33.102 and 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.

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

The authentication and ciphering procedure can be used for either:

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

In 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 (see GSM 03.20 [13]):

- 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
- to let the network set the GSM ciphering mode (ciphering/no ciphering) and GSM ciphering algorithm.

The authentication and ciphering procedure can be used for either:

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

The cases in which the authentication and ciphering procedure shall be used are defined in 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, 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.

******************** NEXT MODIFIED SECTION ********************

4.7.7.2 Authentication and ciphering response by the MS

In GSM, a 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. The calculated 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.

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, GPRS UMTS integrity key and GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous ones. 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.

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~~ use~~d~~ it at an inter system change from UMTS to GSM.

If the AUTHENTICATION AND CIPHERING REQUEST message does not include neither the GSM authentication parameters (RAND and GPRS CKSN) nor the UMTS authentication parameters (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]).

******************** NEXT MODIFIED SECTION ********************

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 AUTHENTICATION AND CIPHERING FAILURE message to the network, with the failure cause 'MAC failure' and parameters provided by the SIM (see TS 33.102).

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 AUTHENTICATION AND CIPHERING FAILURE message to the network, with the failure cause 'Synch failure' and the re-synchronization token AUTS~~parameters~~ provided by the SIM (see TS 33.102).

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

******************** NEXT MODIFIED SECTION ********************

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 10.5.3.1.1~~2~~	O	TLV	18~~16-20~~

9.4.9.1 Authentication Parameter RAND

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

9.4.9.2 GPRS ciphering key sequence number

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

9.4.9.3 Authentication Parameter AUTN

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

9.4.10 Authentication and ciphering response

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

Message type: AUTHENTICATION AND CIPHERING RESPONSE

Significance: dual

Direction: MS to network

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

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Authentication and ciphering response message identity	GPRS message type 10.4	M	V	1
	A&C reference number	A&C reference number 10.5.5.19	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
22	Authentication parameter Response	Authentication Response parameter 10.5.3.2	O	TV	5
23	IMEISV	Mobile identity 10.5.1.4	O	TLV	11
29	Authentication Response parameter (extension)	Authentication Response parameter 10.5.3.2.1	O	TLV	3-14

9.4.10.1 Authentication Response Parameter

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

9.4.10.2 IMEISV

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

9.4.10.3 Authentication Response Parameter (extension)

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

9.4.10a Authentication and Ciphering Failure

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:	AUTHENTICATION AND CIPHERING FAILURE
Significance:	dual
Direction:	mobile station to network

Table 9.4.10a/TS 24.008: 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
	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	Authentication Failure parameter	Authentication Failure parameter 10.5.3.2.2	O	TLV	16~~14 - 18~~

9.4.10a.1 Authentication Failure parameter

This IE shall be sent if and only if the GMM cause was 'Synch failure.' It shall include the response to the authentication challenge from the SIM, which is made up of the AUTS parameter (see TS 33.102).

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

Document ***N1-000785***
revison of N1-000748
revison of N1-000671
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**	**216r2**	Current Version:	3.3.1

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

For submission to:	CN#8	for approval	☒	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: (U)SIM □ ME ☒ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: Siemens AG **Date:** 24.05.2000

Subject: Correction of the MM Authentication procedure

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	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: The length of various authentication parameters was changed by CR 33.102-37r1.

Clauses affected: 4.3.2, 9.2.2, 9.2.3, 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:

help.doc

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

4.3.2 Authentication procedure

4.3.2a Authentication procedure used for a UMTS authentication challenge

The purpose of the authentication procedure is fourfold (see TS 33.102):

First to permit the network to check whether the identity provided by the mobile station is acceptable or not~~ (see 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 mobile station to authenticate the network

The cases where the authentication procedure should be used are defined in TS 33.102~~GSM 02.09~~.

The UMTS 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 UMTS authentication challenge sent by 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 (see GSM 03.20):

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.

******************* NEXT MODIFIED SECTION *******************

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 addition, a GSM ciphering key can be computed from the UMTS ciphering key and the UMTS integrity key by means of an unkeyed conversion function.

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 (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 ciphering key sequence number with the GSM ciphering key (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 and derived GSM ciphering 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, 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, the network may choose to start ciphering with the stored GSM ciphering key (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.

******************** NEXT MODIFIED SECTION ********************

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 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 AUTHENTICATION FAILURE message to the network, with the failure cause 'MAC failure' (see 33.102).

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 AUTHENTICATION FAILURE message to the network, with the failure cause 'Synch failure' and ~~parameters~~ a re-synchronization token AUTS provided by the SIM (see TS 33.102)

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

******************** NEXT MODIFIED SECTION ********************

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 10.5.3.1.1~~2~~	O	TLV	18~~16-20~~

9.2.2.1 Authentication Parameter AUTN

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

9.2.3 Authentication response

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

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: mobile station to network

Table 9.2.4/TS 24.008: AUTHENTICATION RESPONSE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication Response message type	Message type 10.4	M	V	1
	Authentication Response parameter	Auth. Response parameter 10.5.3.2	M	V	4
21	Authenticatio Response Parameter (extension)	Auth. Response parameter 10.5.3.2.1	O	TLV	3-14

9.2.3.1 Authentication Response Parameter

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

9.2.3.2 Authentication Response Parameter (extension)

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

9.2.3a Authentication Failure

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: AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.2.4a/TS 24.008: 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
	Authentication Failure Message type	Message type 10.4	M	V	1
	Reject Cause	Reject Cause 10.5.3.6	M	V	1
22	Authentication Failure parameter	Authentication Failure parameter 10.5.3.2.2	O	TLV	16~~14 - 18~~

9.2.3a.1 Authentication Failure parameter

This IE shall be sent if and only if the reject cause was 'Synch failure.' It shall include the response to the authentication challenge from the SIM, which is made up of the AUTS parameter (see TS 33.102).

******************** NEXT MODIFIED SECTION ********************

10.5.3.1 Authentication parameter RAND

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

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

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

8	7	6	5	4	3	2	1	
Authentication parameter RAND IEI								octet 1
RAND value								octet 2 octet 17

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

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

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

10.5.3.1.1~~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~~length of 18~~16~~ octets~~ and a maximum of 20 octets length~~.

8	7	6	5	4	3	2	1	
Authentication Parameter AUTN IEI								octet 1
Length of AUTN contents								octet 2
AUTN								octet 3
								octet 18~~20~~

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~~18) The AUTN consists of	 (SQN xor AK)||AMF||MAC =~~(32 to 64)~~48+16+64 bits (see TS 33.102)

10.5.3.2 Authentication Response parameter

The purpose of the *authentication response parameter* information element is to provide the network with the authentication response calculated in the SIM.

The *Authentication Parameter SRES* information element is coded as shown in figure 10.5.76/TS 24.008 and tables 10.5.90 a & b /TS 24.008.

The *Authentication Response Parameter* is a type 3 information element with 5 octets length. In a GSM authentication challenge, the response calculated in the SIM (SRES) is 4 bytes in length, and is placed in the *Authentication Response Parameter* information element.

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

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

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

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

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

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

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

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

This IE is included if the authentication response parameter RES is longer than 4 octets (UMTS only) and therefore does not fit in the Authentication Response Parameter field (see 10.5.3.2).

The Authentication Response parameter (extension) IE is coded as shown in figure 10.5.76.1/TS 24.008 and table 10.5.90.1/TS 24.008.

The Authentication Response parameter (extension) IE is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets.

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

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

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

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

10.5.3.2.2 Authentication Failure parameter (UMTS authentication challenge only)

The purpose of the *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 'Synch failure', following a UMTS authentication challenge.

The 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 Authentication Failure parameter IE is a type 4 information element with a ~~minimum~~ length of 16~~14~~ octets~~ and a maximum length of 18 octets~~.

8 7 6 5 4 3 2 1	
Authentication Failure parameter IEI	octet 1
Length ofAuthentication Failure parameter contents	octet 2
Authentication Failure parameter : :	octet 3 octet 16~~18~~

Figure 10.5.76.2/TS 24.008 Authentication Failure parameter information element (UMTS authentication challenge only)

Table 10.5.90.2/TS 24.008: Authentication Failure parameter information element

Authentication Failure parameter value (octet 3 to 16~~18~~) This contains AUTS (see TS 33.102)

3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000337**
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.

33.103 CR xxx 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: SA #8
list expected approval meeting # here ↑

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

Source: Ericsson **Date:** 2000-05-19

Subject: SQN length

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	□
D	Editorial modification	□

Release:

Phase 2	□
Release 96	□
Release 97	□
Release 98	□
Release 99	☒
Release 00	□

Reason for change: S3 decision to fix the length of SQN to 48 bits must be reflected in TS 33.103. The length of “AUTN”, “AUTS” and “UMTS AV” is also aligned accordingly.

Clauses affected: 4.2.2, 4.5.3, 4.6.1

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: This CR considers that EUIC and MAP Security features are not part of R99 and therefore these chapters are not updated and proposed to be removed instead.

help.doc

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

4.2.2 Authentication and key agreement (AKA$_{USIM}$)

The USIM shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored on the USIM:

a) K: a permanent secret key;

b) SQN$_{MS}$: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user;

c) RAND$_{MS}$: the random challenge which was received together with the last AUTN parameter accepted by the user. It is used to calculate the re-synchronisation message together with the highest accepted sequence number (SQN$_{MS}$);

d) KSI: key set identifier;

e) THRESHOLD$_{C}$: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;

f) CK The access link cipher key established as part of authentication;

g) IK The access link integrity key established as part of authentication;

h) HFN$_{MS:}$ Stored Hyper Frame Number provides the Initialisation value for most significant part of COUNT-C and COUNT-I. The least significant part is obtained from the RRC sequence number;

i) AMF: A 16-bit field used Authentication Management. The use and format are unspecified in the architecture but examples are given in an informative annex;

j) The GSM authentication parameter and GSM cipher key derived from the UMTS to GSM conversion functions.

Table 3 provides an overview of the data elements stored on the USIM to support authentication and key agreement.

Table 3: USIM – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN_{MS}	Sequence number counter	1	Updated when AKA protocol is executed	~~32-64~~48 bits	Mandatory
WINDOW (option 1)	Accepted sequence number array	1	Updated when AKA protocol is executed	10 to 100 bits	Optional
LIST (option 2)	Ordered list of sequence numbers received	1	Updated when AKA protocol is executed	32-64 bits	Optional
$RAND_{MS}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	1	Updated when AKA protocol is executed	3 bits	Mandatory
$THRESHOLD_{C}$	Threshold value for ciphering	1	Permanent	32 bits	Optional
CK	Cipher key	1	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1	Updated when AKA protocol is executed	128 bits	Mandatory
$HFN_{MS:}$	Initialisation value for most significant part for COUNT-C and for COUNT-I	1	Updated when connection is released	25 bits	Mandatory
AMF	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory
$RAND_{G}$	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
SRES	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
Kc	GSM cipher Key	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

NOTE 1: HE policy may dictate more than one, the active key signalled using the AMF function.

The following cryptographic functions need to be implemented on the USIM:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;

- f5: a key generating function to derive the anonymity key;
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from Ck and IK (UMTS) to Kc (GSM).

Figure 2 provides an overview of the data integrity, data origin authentication and verification of the freshness by the USIM of the RAND and AUTN parameters received from the VLR/SGSN, and the derivation of the response RES, the cipher key CK and the integrity key IK. Note that the anonymity Key (AK) is optional.

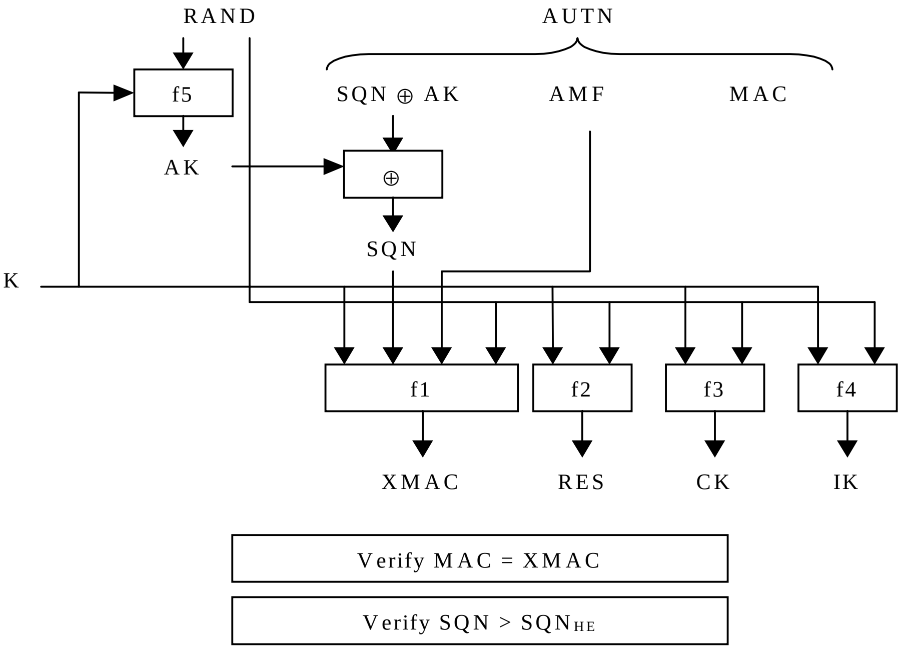


Figure 1: User authentication function in the USIM

Figure 3 provides an overview of the generation in the USIM of a token for re-synchronisation AUTS.

a) The USIM computes MAC-S = $f1*_K(SQN_{MS} \| RAND \| AMF*)$, whereby AMF* is a default value for AMF used in re-synchronisation.

b) If SQN_{MS} is to be concealed with an anonymity key AK, the USIM computes AK = $f5_K(MAC\text{-}S \| 0…0)$, whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter, and the concealed counter value is then computed as $SQN_{MS} \oplus AK$.

c) The re-synchronisation token is constructed as AUTS = SQN_{MS} [$\oplus$ AK] || MAC-S.

Upon receipt of an indication of synchronisation failure and a (AUTS, RAND) pair, the HLR/AuC may perform the following cryptographic functions:

a) If SQN_{MS} is concealed with an anonymity key AK, the HLR/AuC computes AK = $f5_K(MAC\text{-}S \| 0…0)$, whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter and retrieves the unconcealed counter value as $SQN_{MS} = (SQN_{MS} \oplus AK)$ xor AK.

b) If SQN generated from SQN_{HE} would not be acceptable, then the HLR/AuC computes XMAC-S = $f1*_K(SQN_{MS} \| RAND \| AMF*)$, whereby AMF* is a default value for AMF used in re-synchronisation.

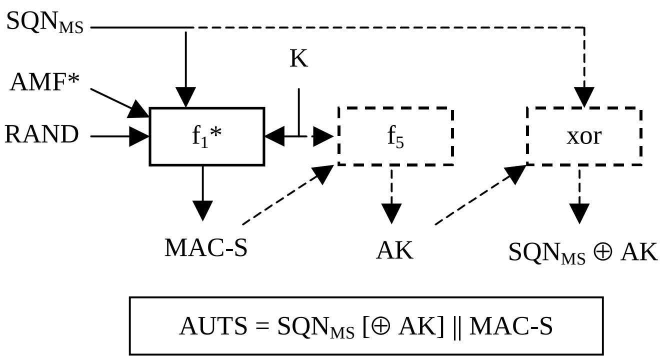


Figure 2: Generation of a token for re-synchronisation AUTS (note 1)

NOTE 1: The lengths of AUTS and MAC-S are specified in table 20~~2~~.

Table 4 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 4: USIM – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function	1	Permanent	Proprietary	Optional
c2 and c3	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	Optional

4.5.3 Authentication and key agreement (AKA_{SN})

The VLR (equivalently the SGSN) shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the VLR (and SGSN):

a) AV: Authentication vectors;

Table 16 provides an overview of the composition of an authentication vector

Table 16: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
RAND	Network challenge	1	128
XRES	Expected response	1	32-128
CK	Cipher key	1	128
IK	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	128~~112-144~~
SQN or SQN ⊕ AK	Sequence number or Concealed sequence number	1 per AUTN	48~~32-64~~
AMF	Authentication Management Field	1 per AUTN	16
MAC-A	Message authentication code for network authentication	1 per AUTN	64

b) KSI: Key set identifier;

c) CK: Cipher key;

d) IK: Integrity key;

e) GSM AV: Authentication vectors for GSM.

Table 17 provides an overview of the data elements stored in the VLR/SGSN to support authentication and key agreement.

Table 17: VLR/SGSN – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UMTS AV	UMTS Authentication vectors	several per user, SN dependent	Depends on many things	528-640~~656~~	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	3 bits	Mandatory
CK	Cipher key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
GSM AV	GSM Authentication vectors	As for GSM	As for GSM	As for GSM	Optional

The following cryptographic functions shall be implemented in the VLR/SGSN:

- c4: Conversion function for interoperation with GSM from Kc (GSM) to CK (UMTS);
- c5: Conversion function for interoperation with GSM from Kc (GSM) to IK (UMTS).

Table 18 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

Table 18: VLR/SGSN Authentication and Key Agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
c4	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional
c5	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.6.1 Authentication and key agreement (AKA$_{he}$)

The HLR/AuC shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the HLR/AuC:

a) K: a permanent secret key;

b) SQN$_{HE}$: a counter used to generate SQN from;

c) AV: authentication vectors computed in advance;

Table 19 provides an overview of the data elements stored on the HLR/AuC to support authentication and key agreement.

Table 19: HLR/AuC – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1	Permanent	128 bits	Mandatory
SQN$_{HE}$	Sequence number counter	1	Updated when AVs are generated	48~~32-64~~ bits	Mandatory
UMTS AV	UMTS Authentication vectors	HE option	Updated when AVs are generated	544-640 bits	Optional
GSM AV	GSM Authentication vectors	HE option that consists of:	Updated when AVs are generated	As GSM	Optional
RAND	GSM Random challenge			128 bits	Optional
SRES	GSM Expected response			32 bits	Optional
Kc	GSM cipher key			64 bits	Optional

Table 20 shows how the construction of authentication token for synchronisation failure messages used to support authentication and key agreement.

Table 20: Composition of an authentication token for synchronisation failure messages

Symbol	Description	Multiplicity	Length
AUTS	Synchronisation Failure authentication token	that consists of:	112~~96–128~~
SQN	Sequence number	1 per AUTS	48~~32-64~~
MAC-S	Message authentication code for Synchronisation Failure messages	1 per AUTS	64

Figure 4 provides an overview of how authentication vectors are generated in the HLR/AuC.

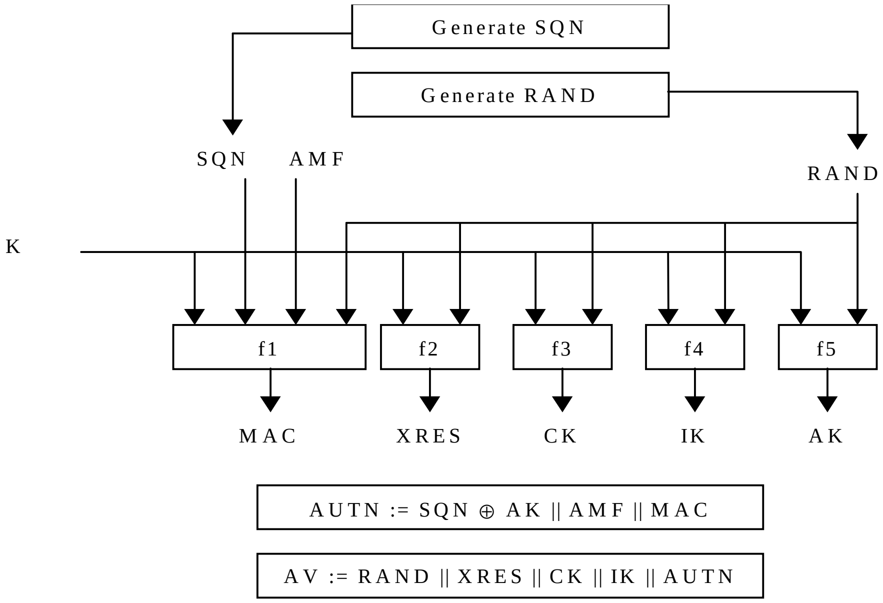

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 3: Generation of an authentication vector

The following cryptographic functions need to be implemented in the HLR/AuC:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key;
- c1: Conversion function for interoperation with GSM from RAND (UMTS) > RAND (GSM);
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from CK and IK (UMTS) to Kc (GSM).

Table 21 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 21: HLR/AuC – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function	1	Permanent	Proprietary	Optional
A3/A8	GSM user authentication functions	1	Permanent	Proprietary	Optional
c1, c2 and c3	Functions for converting UMTS AV's to GSM AV's	1 for each	Permanent	Standard	Optional

3GPP TSG SA WG 3 (Security) meeting #9
Helsinki, 7—9 December 1999

S3-99548

3G CHANGE REQUEST

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

TS 33.102 CR 37r1

Current Version: V3.2.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA#6
list TSG meeting no. here ↑

for approval ☒
for information □
(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf

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

Source: S3 **Date:** 1999-Dec-09

Subject: Authentication and key agreement

3G Work item: Security

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

F	Correction	□
A	Corresponds to a correction in a 2G specification	□
B	Addition of feature	□
C	Functional modification of feature	☒
D	Editorial modification	□

Reason for change: Include requirements on sequence number handling, remove description of any particular method of sequence number handling, improve efficiency of re-synchronisation procedure, correct notation

Clauses affected: Section 6.3

Other specs affected:

Other 3G core specifications	□	→ List of CRs:
Other 2G 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: The value of the number x = 50 in requirement e) in section 6.3.2 shall be used pending further studies.

help.doc

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

6.3 Authentication and key agreement

6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters *SEQ_{MS}* ~~SQN_{MS}~~ and *SEQ_{HE}* ~~SQN_{HE}~~ respectively to support network authentication.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

An overview of the mechanism is shown in figure 4.

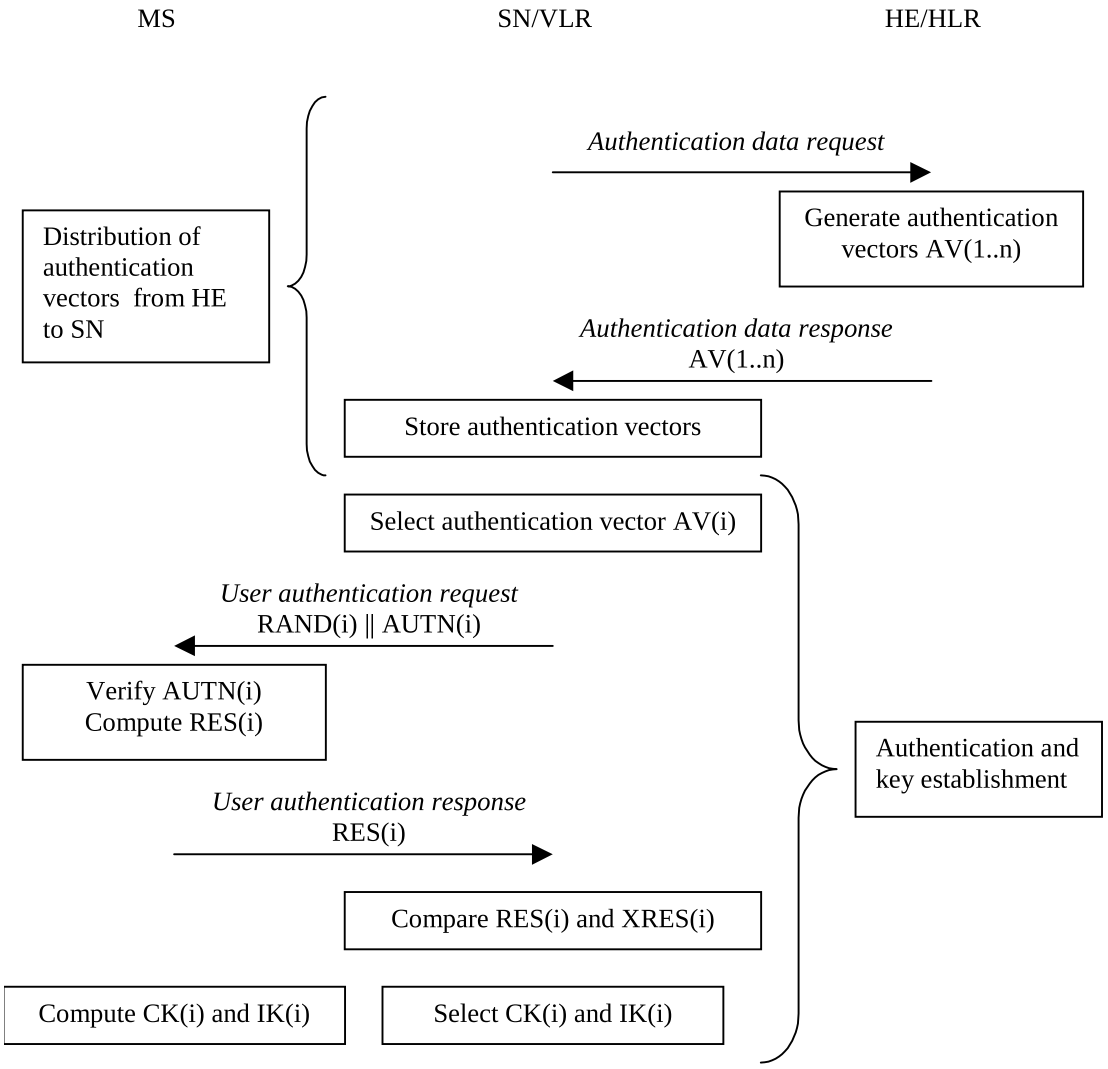

MS
SN/VLR
HE/HLR
Authentication data request
Generate authentication vectors AV(1..n)
Distribution of authentication vectors from HE to SN
Authentication data response AV(1..n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i) Compute RES(i)
Authentication and key establishment
User authentication response RES(i)
Compare RES(i) and XRES(i)
Compute CK(i) and IK(i)
Select CK(i) and IK(i)

Figure 4: Authentication and key agreement

Upon receipt of a request from the ~~SN/VLR~~VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the ~~SN/VLR~~VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the ~~SN/VLR~~VLR/SGSN and the USIM.

When the ~~SN/VLR~~VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the ~~SN/VLR~~VLR/SGSN. The USIM also computes CK and IK. The ~~SN/VLR~~VLR/SGSN compares the received RES with XRES. If they match the ~~SN/VLR~~VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the ~~SN/VLR~~VLR/SGSN to the entities which perform ciphering and integrity functions.

~~SN/VLR~~VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user’s HE (HE/AuC) and the USIM in the user’s mobile station. The mechanism consists of the following procedures:

A procedure to distribute authentication information from the HE/AuC to the ~~SN/VLR~~VLR/SGSN. This procedure is described in 6.3.2. The ~~SN/VLR~~VLR/SGSN is assumed to be trusted by the user’s HE to handle authentication information securely. It is also assumed that the intra-system links between the ~~SN/VLR~~VLR/SGSN to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the ~~SN/VLR~~VLR/SGSN and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited ~~VLR~~VLR/SGSN to the newly visited ~~VLR~~VLR/SGSN. This procedure is described in 6.3.4. It is also assumed that the links between ~~SN/VLR~~VLR/SGSNs are adequately secure. Mechanisms to secure these links are described in clause 7.

6.3.2 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the ~~SN/VLR~~VLR/SGSN with an array of fresh authentication vectors from the user’s HE to perform a number of user authentications.

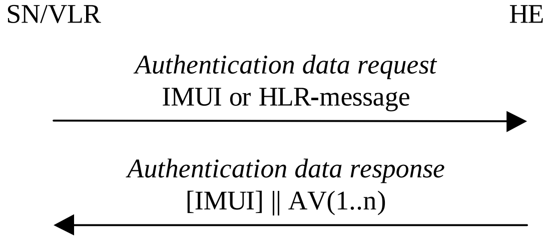


Figure 5: Distribution of authentication data from HE to ~~SN/VLR~~VLR/SGSN

The ~~SN/VLR~~VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC.

The *authentication data request* shall include a user identity. If the user is known in the ~~SN/VLR~~VLR/SGSN by means of the IMUI, the *authentication data request* shall include the IMUI. However, if the user is identified by means of an encrypted permanent identity (see 6.2), the HLR-message from which the HE can derive the IMUI is included instead. In that case, this procedure and the procedure *user identity request to the HLR* are integrated.

Upon the receipt of the *authentication data request* from the ~~SN/VLR~~VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the ~~SN/VLR~~VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n).

Figure 6 shows the generation of an authentication vector AV by the HE/AuC.

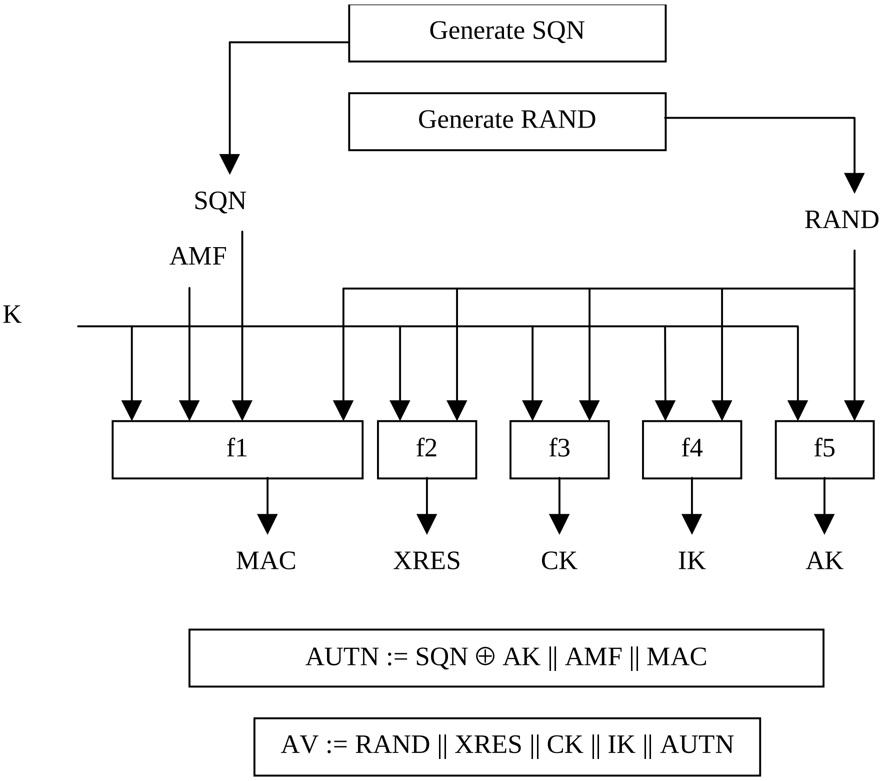

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 6: Generation of an authentication vector

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

For each user the HE/AuC keeps track of a counter~~:~~ SEQ_{HE}~~SQN_{HE} .~~.

~~To generate a fresh sequence number, the counter is incremented and subsequently the SQN is set to the new counter value.~~

~~Note 1:~~ The HE has some flexibility in the management of sequence numbers
, but some requirements need to be fulfilled by the mechanism used:

a) The generation mechanism shall allow a re-synchronisation procedure in the HE described in section 6.3.5

b) The SQN should be generated in such way that it does not expose the identity and location of the user.

c) In case the SQN may expose the identity and location of the user, the AK may be used as an anonymity key to conceal it.

d) The generation mechanism shall allow protection against wrap around the counter in the USIM.
A method how to achieve this is given in informative Annex C.2.

e) The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last x = 50 sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.
~~Such a~~The same minimum number x needs to be ~~defined~~ used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

. ~~Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.~~

The use of SEQ_{HE} is specific to the method of generating sequence numbers. ~~It~~A method is specified in Annex C.1 how to generate a fresh sequence number. A method is specified in Annex C.2 how to verify the freshness of a sequence number.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of this field are included in Annex F.

Subsequently the following values are computed:

- a message authentication code MAC = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;
- an expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;
- a cipher key CK = $f3_K$ (RAND) where f3 is a key generating function;
- an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;
- an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function or f5 ≡ 0.

Finally the authentication token AUTN = SQN ⊕ AK || AMF || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then f5 ≡ 0.

~~Note 1: The need for f5 to use a long-term key different from K is ffs.~~

~~Note 2: The requirements on f3, f4 and f5 are ffs.~~

~~Note 3: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.~~

6.3.3 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the ~~SN/VLR~~VLR/SGSN and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

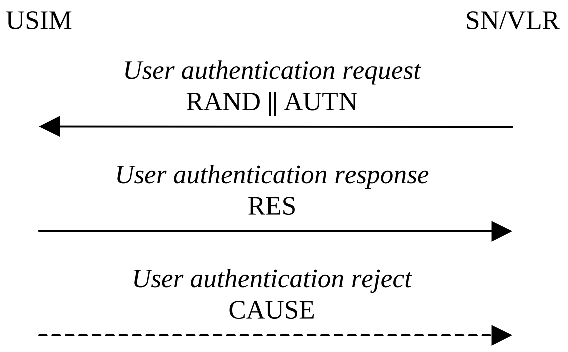

USIM
SN/VLR
User authentication request
RAND || AUTN
User authentication response
RES
User authentication reject
CAUSE

Figure 7: Authentication and key establishment

The ~~SN/VLR~~VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The ~~SN/VLR~~VLR/SGSN sends to the user the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 8.

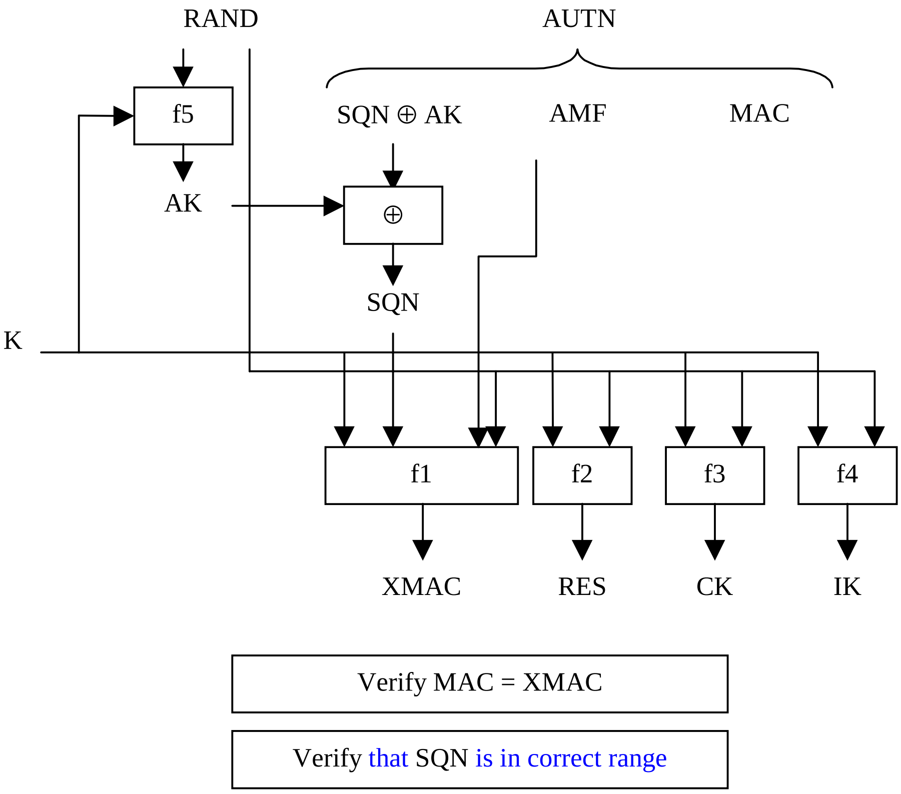


Figure 8: User authentication function in the USIM

Upon receipt of RAND and AUTN the user first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN $\oplus$ AK) $\oplus$ AK.

Next the user computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the ~~SN/VLR~~VLR/SGSN with an indication of the cause and the user abandons the procedure.

Next the ~~user~~ USIM verifies that the received sequence number SQN is ~~in the correct range~~fresh. ~~How the USIM does~~

~~this verification is described in Annex C.2.~~

~~The USIM keeps track of a counter: SQN_{MS}.~~

~~To verify that the sequence number SQN is in the correct range, the USIM compares SQN with SQN_{MS}. If SQN > SQN_{MS} the MS considers the sequence number to be in the correct range and subsequently sets SQN_{MS} to SQN.~~

~~Note: The MS and the HE have some flexibility in the management of sequence numbers. Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.~~

If the user considers the sequence number to be not in the correct range, he sends *synchronisation failure* back to the ~~SN/VLR~~VLR/SGSN including an appropriate parameter, and abandons the procedure.

The *synchronisation failure* message contains the parameter ~~$RAND_{MS}$ ||~~ *AUTS*.
~~Here $RAND_{MS}$ is the random value stored on the MS which was received in user authentication request causing the last update of SQN_{MS} .~~
It is *AUTS = Conc(*SEQ_{MS}~~SQN_{MS}~~*) || MACS.*
Conc(SEQ_{MS}~~SQN_{MS}~~*) =* SEQ_{MS} ~~SQN_{MS}~~ $\oplus f5_K($~~$RAND_{MS}$~~*MACS)* is the concealed value of the counter SEQ_{MS} ~~SQN_{MS}~~ in the MS, and.
MACS = $f1^*_K($$SEQ_{MS}$ ~~SQN_{MS}~~ *|| RAND || AMF)* where *RAND* is the random value received in the current user authentication request.
f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 9:

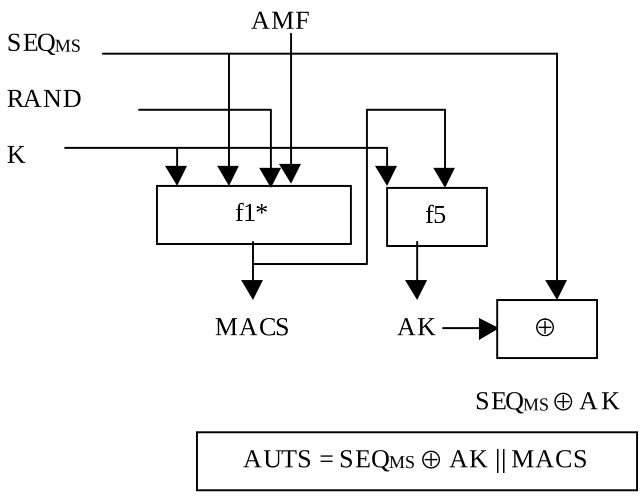


Figure 9: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the user computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the ~~SN/VLR~~VLR/SGSN. Finally the user computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. The MS stores RAND for re-synchronisation purposes.

Upon receipt of *user authentication response* the ~~SN/VLR~~VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The ~~SN/VLR~~VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector.

Conditions on the use of authentication information by the ~~SN/VLR~~VLR/SGSN: ~~Using the procedures described in subsections 6.3.1, 6.3.2 and 6.3.4, authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt.~~ The ~~SN/VLR~~**VLR/SGSN** shall use an authentication vector only once and, hence, shall send out each user authentication request *RAND* || *AUTN* only once no matter whether the authentication attempt was successful or not. A consequence is that authentication vectors cannot be reused. ~~When a user changes from one VLR to another one and the new VLR requests remaining authentication vectors from the old VLR (cf. subsection 6.3.4) then the old VLR shall not retain any copies of these authentication vectors. When a VLR receives a "cancel location" request for a certain user it shall delete all authentication vectors relating to that user. When a VLR receives a location update request from a user and the VLR notices that authentication vectors relating to that user are still stored in the VLR it will delete this information and request fresh authentication vectors from the HE/AuC.~~

~~Different rules may apply when one of the alternative schemes for sequence number handling described in Annex C or Annex F.3 are applied. This is true in particular when the schemes based on windows or lists described in Annexes C.3 and C.4 are applied.~~

6.3.3.1 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network service domains. The conditions on the use of these cipher keys in the user and control planes are given below.

6.3.3.1.1 User plane

The CS user data connections are ciphered with the cipher key CK_{CS} established between the user and the 3G CS core network service domain and identified in the security mode setting procedure. The PS user data connections are ciphered with the cipher key CK_{PS} established between the user and the 3G PS core network service domain and identified in the security mode setting procedure.

6.3.3.1.2 Control plane

When a security mode setting procedure is performed, the cipher/integrity key set by this procedure is applied to the signalling plane, what ever core network service domain is specified in the procedure. This may require that the cipher/integrity key of an (already ciphered/integrity protected) ongoing signalling connection is changed. This change should be completed within five seconds.

6.3.4 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR.

The procedure is shown in Figure 10.

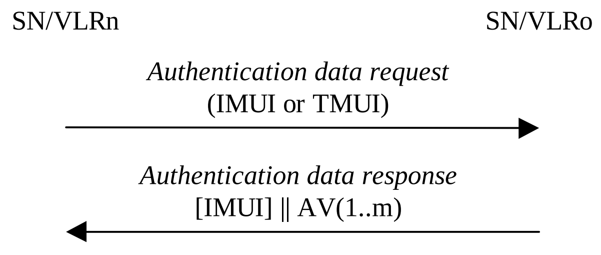


Figure 10: Distribution of authentication data between ~~SN/VLR~~VLR/SGSN

The procedure is invoked by the newly visited ~~SN/VLR~~**VLR/SGSN**n after a *location update request* sent by the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of ~~SN/VLR~~**VLR/SGSN**o. In that case this procedure is integrated with the procedure described in 6.1.4.

Upon receipt of the request the VLRo verifies whether it has any unused authentication vectors of the appropriate mode in its database and if so, sends the unused authentication vectors to VLRn. The previously visited VLRo shall then delete these authentication vectors from its database.

Upon receipt the VLRn stores the received authentication vectors.

If VLRo indicates that it has no authentication vectors or the VLRo cannot be contacted, VLRn should request new authentication vectors from the user's HE using the procedure described in 6.3.2.

6.3.5 Re-synchronisation procedure

An ~~SN/VLR~~**VLR/SGSN** may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the ~~SN/VLR~~**VLR/SGSN** sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- ~~$RAND_{MS}$ ||~~ *AUTS* received by the ~~SN/VLR~~**VLR/SGSN** in the response to that request, as described in subsection 6.3.3.

An ~~SN/VLR~~**VLR/SGSN** will not react to unsolicited " synchronisation failure indication" messages from the MS.

The ~~SN/VLR~~**VLR/SGSN**VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

(1)~~-~~The HE/AuC retrieves SEQ_{MS} from Conc(SEQ_{MS}) by computing $f5_K$(*MACS*)~~,~~.

(2) The HE/AuC checks if SEQ_{HE} is in the correct range, i.e. if the next sequence number generated SEQ_{HE} using would be accepted by the USIM.~~ $SEQ_{MS} < SEQ_{HE} < SEQ_{MS} + \Delta$ where the parameters SEQ_{MS} , SEQ_{HE} and Δ are defined in Annex C.~~

(3) If SEQ_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).

(4) The HE/AuC verifies ~~*AUTS* by computing $f5_K(RAND_{MS})$, retrieving SQN_{MS} from Conc(SQN_{MS}) and verifying~~ *MACS* (cf. subsection 6.3.3.).

(5) If the verification is successful~~, but SQN_{MS} is such that SQN_{HE} is not in the correct range then the~~ the HE/AuC resets the value of the counter SEQ_{HE} ~~SQN_{HE}~~ to SEQ_{MS}~~SQN_{MS}~~.

~~Otherwise, the HE/AuC leaves SQN_{HE} unchanged.~~

(6) ~~In all cases the~~ The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the ~~SN/VLR~~VLR/SGSN.

If the counter SEQ_{HE}~~SQN_{HE}~~ was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SEQ_{HE}~~SQN_{HE}~~. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the ~~SN/VLR~~VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an *authentication data request* with synchronisation failure indication it deletes the old ones for that user in the ~~VLR~~VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC.

~~Optionally, in order to minimise extra effort by the HE/AuC, in an authentication data request with synchronisation failure indication the SN/VLR may also send the concealed sequence number Conc(SQN_{SN}) corresponding to the last authentication vector received which the SN/VLR has in storage, i.e. it may send Conc(SQN_{SN}) = $RAND_{SN} \| SQN_{SN} \oplus f5_K(RAND_{MS})$.~~

~~On receipt the HE/AuC retrieves SQN_{SN} from Conc(SQN_{SN}). If the counter in the HE/AuC did not have to be reset and if $SQN_{SN} = SQN_{HE}$ the HE/AuC informs the SN/VLR accordingly and does not send fresh authentication vectors. (In this way, a synchronisation failure does not cause the HE/AuC to produce extra authentication vectors when they are not needed.)~~

Figure 11 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in subclause 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response (*as described in this subclause*).*

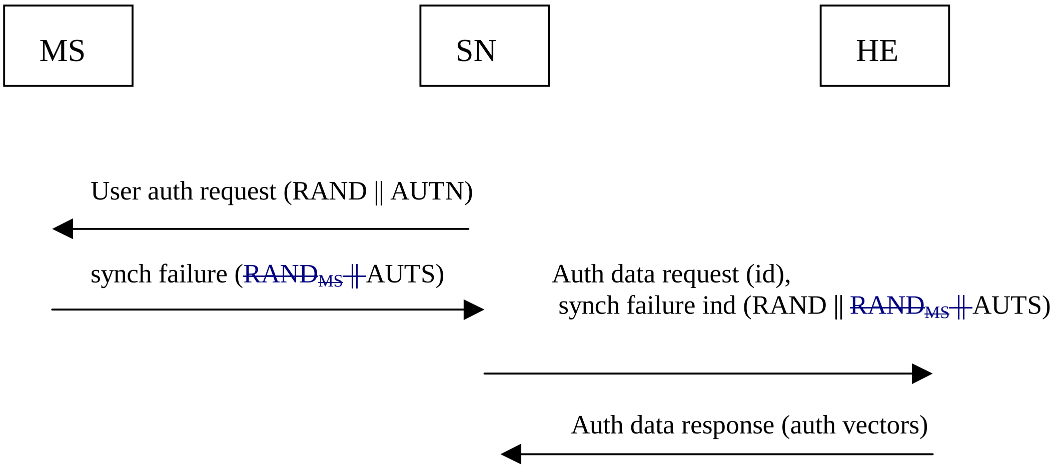

MS
SN
HE
User auth request (RAND || AUTN)
synch failure (~~RAND$_{MS}$ ||~~AUTS)
Auth data request (id),
synch failure ind (RAND || ~~RAND$_{MS}$ ||~~AUTS)
Auth data response (auth vectors)

Figure 11: Re-synchronisation procedure

6.3.6 Length of sequence numbers

Sequence numbers ~~shall~~ shall have a length of 6 octets. ~~be sufficiently long so that they cannot wrap around during the lifetime of the system. Consequently, in normal operations neither SQN$_{MS}$ nor SQN$_{HE}$ can wrap around during the lifetime of a USIM.~~

~~Note 1: If the counters would derive sequence numbers from time (see Annex C), then a 32-bit counter that is derived from the number of seconds that have elapsed since January 1, 2000 would only wrap around in the year 2136. So a length of 32-bits for the sequence numbers and counters should be sufficient. For individual incremental counters, a smaller range of sequence numbers should be sufficient, as authentication and key agreement is expected to occur far less frequently than once every second. Shorter lengths would however exclude the use of time-derived sequence numbers.~~

~~Note 2: Sequence numbers for CS and PS operation are expected to have the same length.~~

~~6.3.7 Support for window and list mechanisms~~

~~In Annex C.3 and Annex C.4 respectively, the window and list mechanisms for sequence number management in the USIM are described. If one of these mechanisms is employed in the USIM and if there is no need to conceal sequence numbers then the MS shall send information on the current value of the lowest entry SQN$_{LO}$ in the window or list to the SN/VLR at every location update. Sequence numbers which do not need to be concealed may be generated according to Annex C.2 or Annex C.6.~~

~~When the SN/VLR authenticates a user for the first time after receiving a new value SQN$_{LO}$ from the MS then the SN/VLR checks whether the sequence number of the authentication vector it wants to use is greater than SQN$_{LO}$. The SN/VLR uses the AV only if this is the case. Otherwise, the AV is discarded. If all AVs have to be discarded the SN/VLR requests new ones from the HE/AuC.~~