3GPP TSG CN Plenary
Meeting #11, Palm Springs, U.S.A
14th - 16th March 2001

Tdoc NP-010127

Source:	**TSG CN WG1**
Title:	**CRs to R99 on Work Item Security**
Agenda item:	**8.14**
Document for:	**APPROVAL**

Introduction:

This document contains **2** CRs on **R99** Work Item **" Security"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #11 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
24.008	280	4	N1-010217	R99	Optional support of UMTS AKA by a GSM only R99 ME	F	3.6.0
24.008	281	4	N1-010218	Rel-4	Optional support of UMTS AKA by a GSM only R99 ME	A	4.1.1

CR-Form-v3

CHANGE REQUEST

	⌘	**24.008** CR **280**	⌘	rev	**4**	⌘	Current version:	**3.6.0**	⌘

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

Proposed change affects: ⌘   (U)SIM ☐   ME/UE **X**   Radio Access Network ☐   Core Network **X**

Title:	⌘	Optional support of UMTS AKA by a GSM only R99 ME
Source:	⌘	Ericsson, Siemens AG, Nokia
Work item code:	⌘	Security	***Date:*** ⌘	2001-01-09
Category:	⌘	**F**	***Release:*** ⌘	R99

	Use one of the following categories:	*Use one of the following releases:*
	F *(essential correction)*	*2* *(GSM Phase 2)*
	A *(corresponds to a correction in an earlier release)*	*R96* *(Release 1996)*
	B *(Addition of feature),*	*R97* *(Release 1997)*
	C *(Functional modification of feature)*	*R98* *(Release 1998)*
	D *(Editorial modification)*	*R99* *(Release 1999)*
	Detailed explanations of the above categories can	*REL-4* *(Release 4)*
	be found in 3GPP TR 21.900.	*REL-5* *(Release 5)*

Reason for change:	⌘	With the LS in Tdoc N1-001163 (S3-000629), S3 has agreed that GSM only R99 ME's are not mandated to support USIMs. This CR aligns 24.008 with the S3 descision.
Summary of change:	⌘	This CR proposes to change the text in 24.008 to say that: UMTS authentication challenge *may* be supported by a ME supporting only GSM radio access, in it clarifies the MS behaviour in this case.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.3.2a, 4.3.2.2, 4.3.2.5.1, 4.7.7a, 4.7.7.2

Other specs affected:	⌘	☐ Other core specifications ⌘	
		☐ Test specifications	
		☐ O&M Specifications	

Other comments:	⌘	

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 3GPP TS 33.102):

First to permit the network to check whether the identity provided by the mobile station is acceptable or not;

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 3GPP TS 33.102.

The UMTS authentication procedure is always initiated and controlled by the network. However, 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 MS~~E~~ supporting <u>the UMTS authentication algorithm</u>~~GSM or UMTS radio access~~.

<u>Note: According to TS 33.102, a ME supporting only A/Gb mode need not support the USIM interface and in consequence need not support the UMTS authentication algorithm.</u>

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;

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

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

The authentication procedure is always initiated and controlled by the network. GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

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

4.3.2.1   Authentication request by the network

The network initiates the authentication procedure by transferring an AUTHENTICATION REQUEST message across the radio interface and starts the timer T3260. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see GSM 03.20 (in case of GSM authentication challenge) and 3GPP TS 33.102 (in case of an UMTS authentication challenge)). In a GSM authentication challenge, the AUTHENTICATION REQUEST message also contains the GSM ciphering ~~ciphering~~ key sequence number allocated to the key which may be computed from the given parameters. In a UMTS authentication challenge, the AUTHENTICATION REQUEST message also contains the ciphering key sequence number allocated to the key set of UMTS ciphering key, UMTS integrity key and GSM ciphering key which may be computed from the given parameters.

4.3.2.2   Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. With exception of the cases described in 4.3.2.5.1, it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION REQUEST message and shall proceed as in case of a GSM authentication challenge. It shall not perform the authentication of the network described in 4.3.2.5.1.

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

In a UMTS authentication challenge, the new UMTS ciphering key, the new GSM ciphering key and the new UMTS integrity key calculated from the challenge information shall overwrite the previous UMTS ciphering key, GSM ciphering key and UMTS integrity key. The new UMTS ciphering key, GSM ciphering key and UMTS integrity key are stored on the SIM together with the ciphering key sequence number.

The SIM will provide the mobile station with the authentication response, based upon the authentication challenge given from the ME~~from the network~~. A UMTS authentication challenge will result in the SIM passing a RES to the ME. A GSM authentication challenge will result in the SIM passing a SRES to the ME.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20 in case of a GSM authentication challenge respective 3GPP TS 33.102 in case of an UMTS authentication challenge).

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

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, 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 3GPP TS 33.102) if the stored ciphering key sequence number and the one given from the mobile station are equal.

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

4.3.2.5   Authentication not accepted by the network

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

-    the TMSI was used;

-    the IMSI was used.

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

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in section 3.5.of 04.18 (GSM) or in 3GPP TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow section 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5.1   Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

~~A R99 GSM- only MS connected to a R99 core network (even using the 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 3GPP 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 reject cause 'MAC failure'. 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 reject cause 'Synch failure' and a re-synchronization token AUTS provided by the SIM (see 3GPP TS 33.102). The MS shall then follow the procedure described in section 4.3.2.6 (d).

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 send the IDENTITY RESPONSE message.

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 T3214, if running, and then process the challenge information as normal.
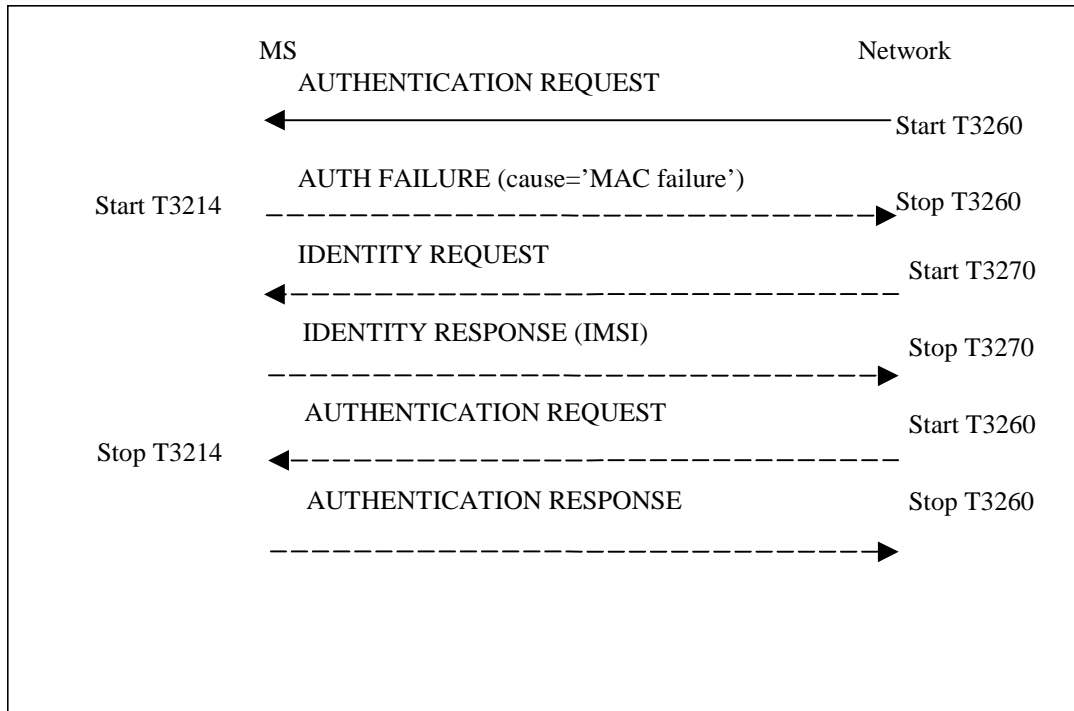
When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).

Upon successfully validating the network (an AUTHENTICATION REQUEST that contains a valid MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230) , if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC.

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 expires;

- Upon receipt of the second AUTHENTICATION REQUEST while T3214 is running and the MAC value cannot be resolved.

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

Figure 4.2/3GPP TS 24.008: Authentication Failure Procedure (reject cause 'MAC failure')

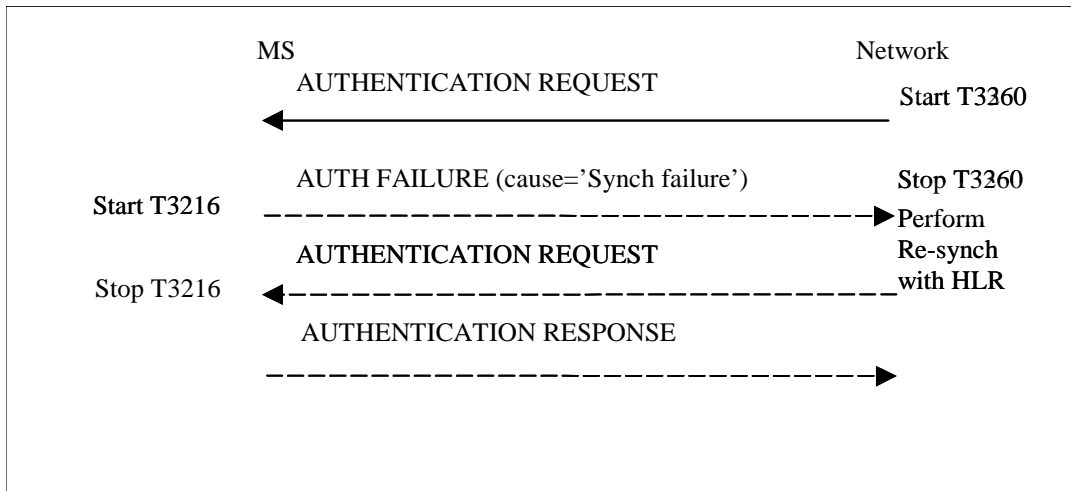(d) Authentication failure (reject cause 'synch failure'):

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.

When the first AUTHENTICATION REQUEST message containing an invalid SQN 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 (a second AUTHENTICATION REQUEST is received which contains a valid SQN) while T3216 is running, the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid SQN.

If the MS receives a second AUTHENTICATION REQUEST which contains an invalid SQN while T3216 is running, then the MS shall behave as described in section 4.3.2.6.1.

If the timer T3216 expires, then the MS shall behave as described in section 4.3.2.6.1.

```
MS                                          Network
        AUTHENTICATION REQUEST            Start T3360
    ◄─────────────────────────────────────

        AUTH FAILURE (cause='Synch failure')   Stop T3360
Start T3216 ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►Perform
                                               Re-synch
        AUTHENTICATION REQUEST                 with HLR
Stop T3216 ◄─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─

        AUTHENTICATION RESPONSE

    ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►
```

Figure 4.2a/3GPP TS 24.008: Authentication Failure Procedure (reject cause 'Synch 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 cell where the AUTHENTICATION REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or SQN.

4.7.7   Authentication and ciphering procedure

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

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

- to permit the network to check whether the identity provided by the MS is acceptable or not;

- to provide parameters enabling the MS to calculate a new GPRS UMTS ciphering key and a new GPRS UMTS integrity key.

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

- to permit the mobile station to authenticate the network.

In 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 3GPP 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 M~~S~~E supporting <u>UMTS authentication algorithm.</u>~~GSM or UMTS radio access.~~

> <u>Note: According to TS 33.102, a ME supporting only A/Gb mode need not support the USIM interface and in consequence need not support the UMTS authentication challenge.</u>

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;

- 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.

4.7.7.1   Authentication and ciphering initiation by the network

The network initiates the authentication and ciphering procedure by transferring an AUTHENTICATION AND CIPHERING REQUEST message across the radio interface and starts timer T3360. The AUTHENTICATION AND CIPHERING REQUEST message shall contain all parameters necessary to calculate the response parameters when authentication is performed (see GSM 03.20 [13] and 3GPP TS 33.102).

If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain either:

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

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

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

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

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

Additionally, the network may request the MS to include its IMEISV in the AUTHENTICATION AND CIPHERING RESPONSE message.

4.7.7.2   Authentication and ciphering response by the MS

In GSM, a 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.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION AND CIPHERING REQUEST message and perform the GSM authentication challenge. It shall not perform the authentication of the network described in 4.7.7.5.1.

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 use 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]).

4.7.7.3   Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see GSM 03.20 [13] and 3GPP TS 33.102). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent.

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

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

4.7.7.4   GPRS 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 GPRS GSM ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the GPRS UMTS ciphering key and the GPRS UMTS integrity key can be computed given the secret key associated to the IMSI.

In order to allow start of ciphering on a logical link without authentication, GPRS ciphering key sequence numbers are introduced.

The GPRS ciphering key sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the GPRS ciphering key sequence number allocated to the GPRS GSM ciphering key (in case of a GSM authentication challenge) or the GPRS UMTS ciphering key and the GPRS UMTS integrity key (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.

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

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

In UMTS, the network may choose to start ciphering and integrity checking with the stored GPRS UMTS ciphering key and the stored GPRS UMTS integrity key (under the restrictions given in GSM 02.09 and 3GPP TS 33.102) if the stored GPRS ciphering key sequence number and the one given from the MS are equal.

In GSM, the network may choose to start ciphering with the stored GPRS GSM ciphering key (under the restrictions given in GSM 02.09) if the stored GPRS ciphering key sequence number and the one given from the MS are equal and the previously negotiated ciphering algorithm is known and supported in the network. When ciphering is requested at GPRS attach, the authentication and ciphering procedure shall be performed since the MS does not store the ciphering algorithm at detach.

Upon GPRS attach, if ciphering is to be used, an AUTHENTICATION AND CIPHERING REQUEST message shall be sent to the MS to start ciphering.

If the GPRS ciphering key sequence number stored in the network does not match the GPRS ciphering key sequence number received from the MS in the ATTACH REQUEST message, then the network should authenticate the MS.

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

In UMTS, the MS starts ciphering and integrity checking according to the conditions specified in specification 3GPP TS 25.331.

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

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

4.7.7.5   Authentication not accepted by the network

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

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

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

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

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310, T3317 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

4.7.7.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see 3GPP 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 GMM cause 'MAC failure'. 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 GMM cause 'Synch failure' and the re-synchronization token AUTS provided by the SIM (see 3GPP TS 33.102). The MS shall then follow the procedure described in section 4.7.7.6 (g).

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.
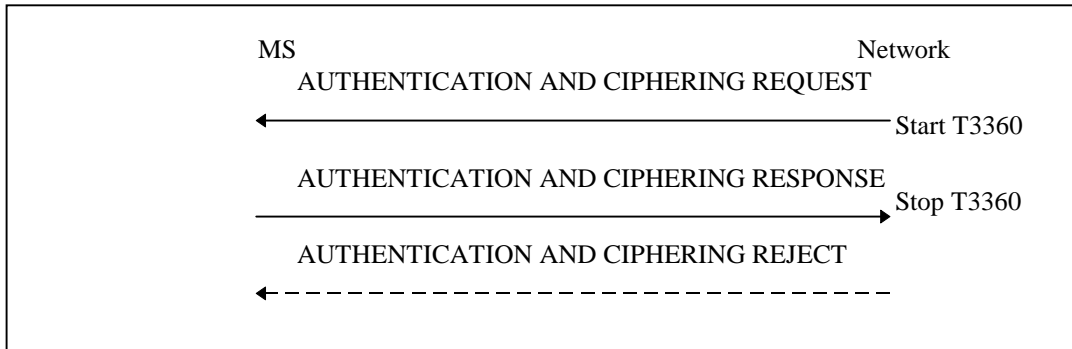
```
MS                                                        Network
          AUTHENTICATION AND CIPHERING REQUEST
    ◄─────────────────────────────────────────────── Start T3360

          AUTHENTICATION AND CIPHERING RESPONSE
    ───────────────────────────────────────────────► Stop T3360

          AUTHENTICATION AND CIPHERING REJECT
    ◄─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─
```

Figure 4.7.7/1 3GPP 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 send the IDENTITY RESPONSE message.

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 T3318, if running, and then process the challenge information as normal.
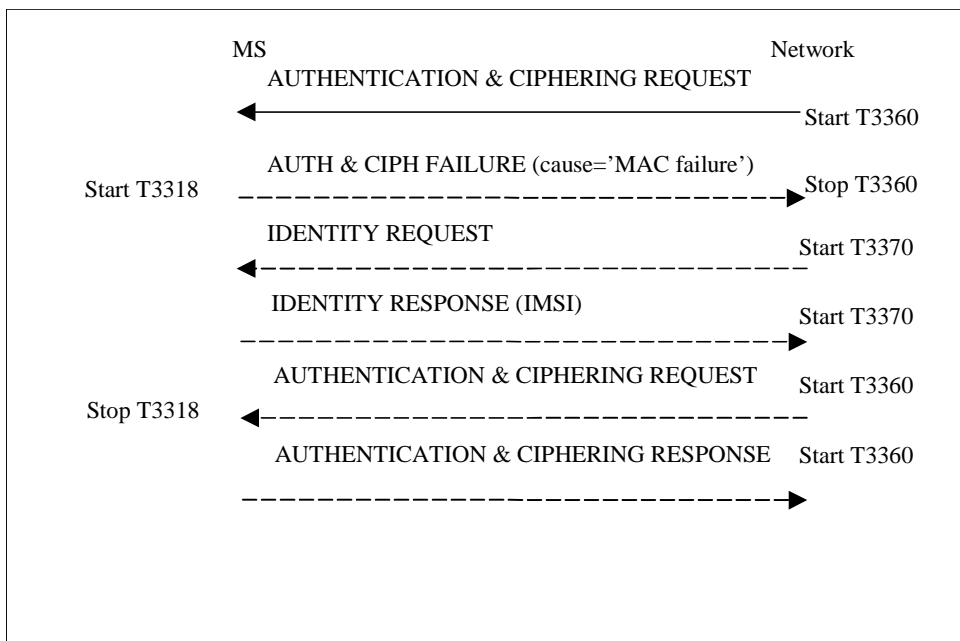
When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

Upon successfully validating the network, (an AUTHENTICATION & CIPHERING REQUEST message that contains a valid MAC is received), the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317) , if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC.

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 expires;

-   Upon receipt of the second AUTHENTICATION & CIPHERING REQUEST message from the network while the T3318 is running and the MAC value 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.

Figure 4.7.7a/1 3GPP TS 24.008: Authentication failure cause 'MAC failure'

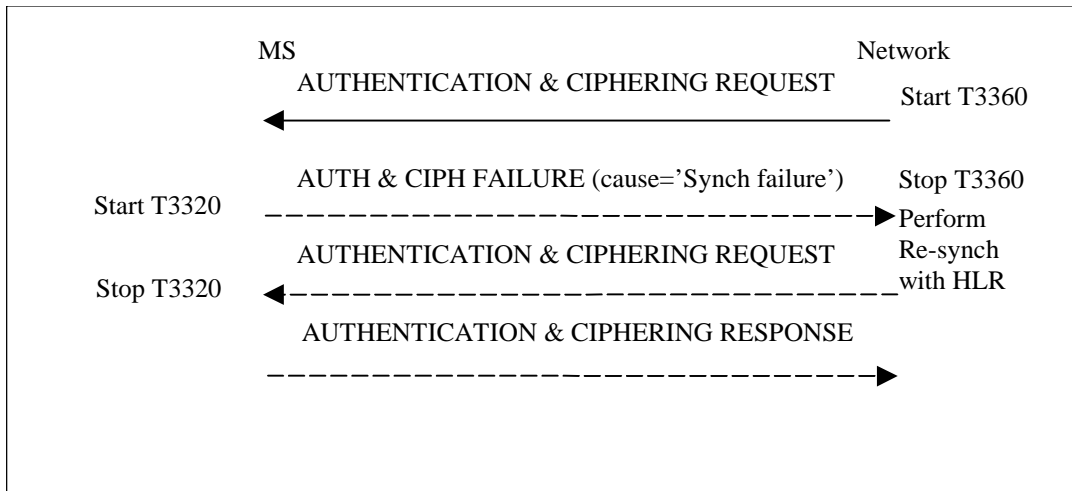(g) Authentication failure (GMM cause 'Synch failure'):

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.

When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid SQN 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, (a second AUTHENTICATION & CIPHERING REQUEST message is received which contains a valid SQN) while T3320 is running, the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid SQN.

If the MS receives a second AUTHENTICATION & CIPHERING REQUEST message which contains an invalid SQN while T3320 is running, then the MS shall behave as described in section 4.7.7.6.1.

If the timer T3320 expires, 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
                  AUTHENTICATION & CIPHERING REQUEST      Re-synch
  Stop T3320   ◄┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈  with HLR

                  AUTHENTICATION & CIPHERING RESPONSE
               ┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈┈►
```

Figure 4.7.7b/1 3GPP TS 24.008: Authentication failure cause 'Synch failure'

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 cell where the AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or SQN.

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	O	TLV	18

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.

The MS shall ignore the IE if it does not support UMTS authentication algorithm.

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	Authentication 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))

This IE shall not be included if MS does not support UMTS authentication algorithm.

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	O	TLV	18

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.

The MS shall ignore the IE if it does not support UMTS authentication algorithm.

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))

This IE shall not be included if MS does not support UMTS authentication algorithm.

CR-Form-v3

CHANGE REQUEST

| ⌘ | **24.008** CR **281** | ⌘ | rev | **4** | ⌘ | Current version: | **4.1.1** | ⌘ |

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title: ⌘	Optional support of UMTS AKA by a GSM only R99 ME	
Source: ⌘	Ericsson, Siemens AG, Nokia	
Work item code: ⌘	Security	*Date:* ⌘ 2001-01-19
Category: ⌘ **A**		*Release:* ⌘ R4

Use <u>one</u> of the following categories:	Use <u>one</u> of the following releases:
F *(essential correction)*	2 *(GSM Phase 2)*
A *(corresponds to a correction in an earlier release)*	R96 *(Release 1996)*
B *(Addition of feature),*	R97 *(Release 1997)*
C *(Functional modification of feature)*	R98 *(Release 1998)*
D *(Editorial modification)*	R99 *(Release 1999)*
Detailed explanations of the above categories can	REL-4 *(Release 4)*
be found in 3GPP TR 21.900.	REL-5 *(Release 5)*

Reason for change: ⌘	With the LS in Tdoc N1-001163 (S3-000629), S3 has agreed that GSM only R99 ME's are not mandated to support USIMs. This CR aligns 24.008 with the S3 descision.
Summary of change: ⌘	This CR proposes to change the text in 24.008 to say that: UMTS authentication challenge *may* be supported by a ME supporting only GSM radio access, in it clarifies the MS behaviour in this case.
Consequences if ⌘ *not approved:*	

Clauses affected: ⌘	4.3.2a, 4.3.2.2, 4.3.2.5.1, 4.7.7a, 4.7.7.2
Other specs ⌘ *affected:*	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments: ⌘	

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;

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.

The UMTS authentication procedure is always initiated and controlled by the network. However, 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 MSE supporting the ~~USIM interface GSM~~UMTS authentication algorithm~~GSM or UMTS radio access~~.

Note: According to TS 33.102, a ME supporting only A/Gb mode need not support the USIM interface and in consequence need not support the UMTS authentication algorithm.

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;

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

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

The authentication procedure is always initiated and controlled by the network. GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

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

4.3.2.1   Authentication request by the network

The network initiates the authentication procedure by transferring an AUTHENTICATION REQUEST message across the radio interface and starts the timer T3260. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see GSM 03.20 (in case of GSM authentication challenge) and TS 33.102 (in case of an UMTS authentication challenge)). In a GSM authentication challenge, the AUTHENTICATION REQUEST message also contains the GSM ciphering ~~ciphering~~ key sequence number allocated to the key which may be computed from the given parameters. In a UMTS authentication challenge, the AUTHENTICATION REQUEST message also contains the ciphering key sequence number allocated to the key set of UMTS ciphering key, UMTS integrity key and GSM ciphering key which may be computed from the given parameters.

4.3.2.2   Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. With exception of the cases described in 4.3.2.5.1, it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION REQUEST message and shall proceed as in case of a GSM authentication challenge. It shall not perform the authentication of the network described in 4.3.2.5.1.

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

In a UMTS authentication challenge, the new UMTS ciphering key, the new GSM ciphering key and the new UMTS integrity key calculated from the challenge information shall overwrite the previous UMTS ciphering key, GSM ciphering key and UMTS integrity key. The new UMTS ciphering key, GSM ciphering key and UMTS integrity key are stored on the SIM together with the ciphering key sequence number.

The SIM will provide the mobile station with the authentication response, based upon the authentication challenge given from the ME~~from the network~~. A UMTS authentication challenge will result in the SIM passing a RES to the ME. A GSM authentication challenge will result in the SIM passing a SRES to the ME.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20 in case of a GSM authentication challenge respective TS 33.102 in case of an UMTS authentication challenge).

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

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, 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.

4.3.2.5   Authentication not accepted by the network

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

-    the TMSI was used;

-    the IMSI was used.

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

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in section 3.5.of 04.18 (GSM) or in TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow section 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5.1   Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

~~A R99 GSM-only MS connected to a R99 core network (even using the 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 reject cause 'MAC failure'.
      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 reject cause 'Synch failure'
      and a re-synchronization token AUTS provided by the SIM (see TS 33.102). The MS shall then follow the
      procedure described in section 4.3.2.6 (d).

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 send the IDENTITY RESPONSE message.

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 T3214, if running, and then process the challenge information as normal.
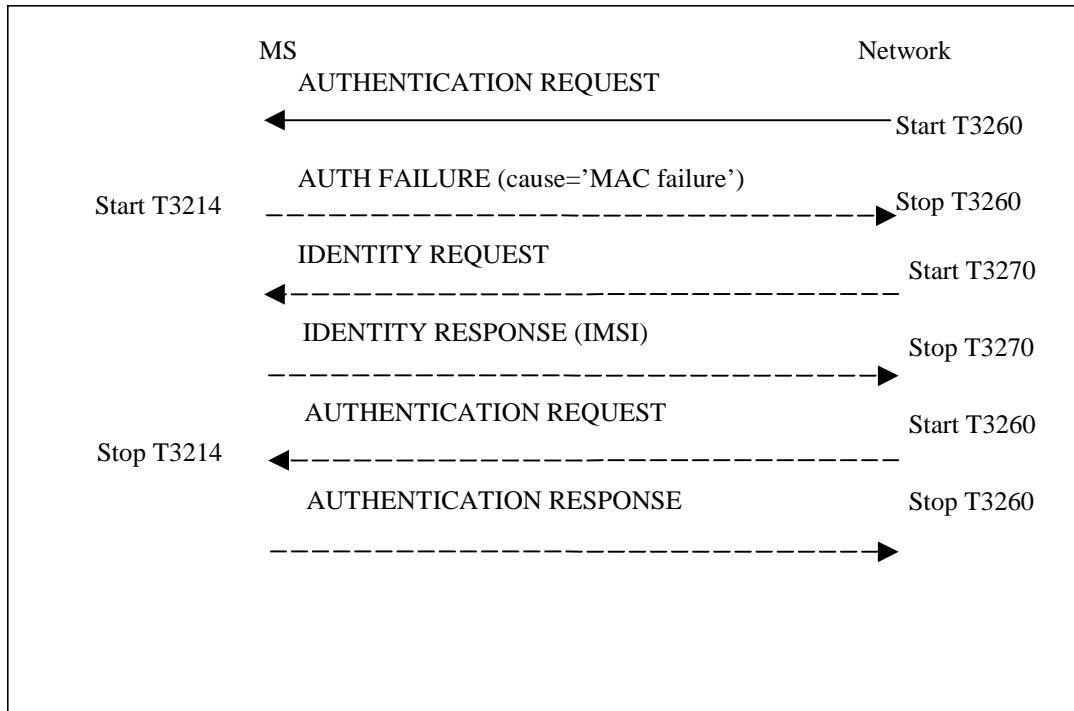
When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).

Upon successfully validating the network (an AUTHENTICATION REQUEST that contains a valid MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230) , if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC.

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 expires;

-   Upon receipt of the second AUTHENTICATION REQUEST while T3214 is running and the MAC value cannot be resolved.

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

```
                    MS                                    Network
                         AUTHENTICATION REQUEST
                                                              Start T3260
                     ◄─────────────────────────────────

                         AUTH FAILURE (cause='MAC failure')
    Start T3214      ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►  Stop T3260

                         IDENTITY REQUEST
                                                              Start T3270
                     ◄─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─

                         IDENTITY RESPONSE (IMSI)
                                                              Stop T3270
                     ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►

                         AUTHENTICATION REQUEST
                                                              Start T3260
    Stop T3214       ◄─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─

                         AUTHENTICATION RESPONSE
                                                              Stop T3260
                     ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►
```

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

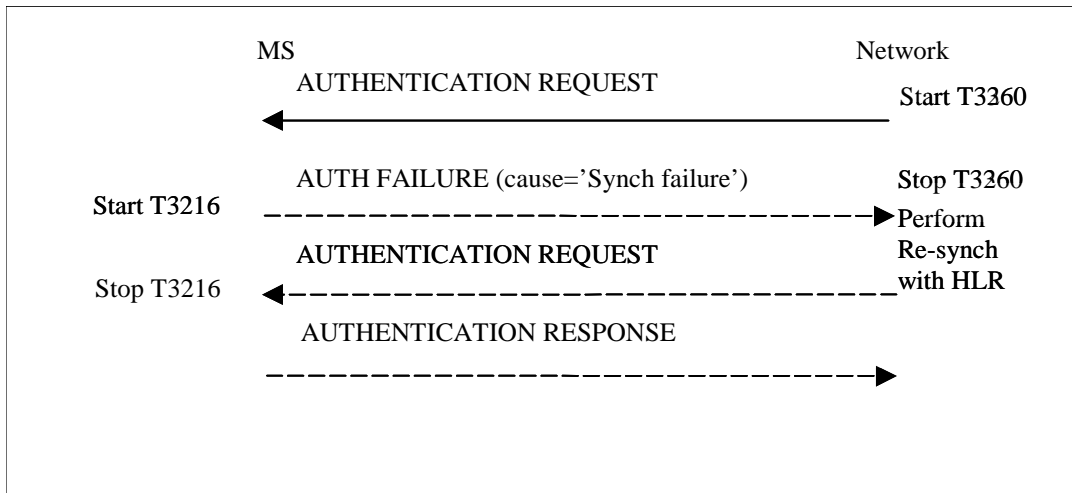(d) Authentication failure (reject cause 'synch failure'):

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.

When the first AUTHENTICATION REQUEST message containing an invalid SQN 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 (a second AUTHENTICATION REQUEST is received which contains a valid SQN) while T3216 is running, the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid SQN.

If the MS receives a second AUTHENTICATION REQUEST which contains an invalid SQN while T3216 is running, then the MS shall behave as described in section 4.3.2.6.1.

If the timer T3216 expires, then the MS shall behave as described in section 4.3.2.6.1.

Figure 4.2a/TS 24.008: Authentication Failure Procedure (reject cause 'Synch 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 cell where the AUTHENTICATION REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or SQN.

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;

-   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 M~~S~~E supporting UMTS authentication algorithm .~~GSM or UMTS radio access.~~

   Note: According to TS 33.102, a ME supporting only A/Gb mode need not support the USIM interface and in consequence need not support the UMTS authentication challenge.

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;

-   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.

4.7.7.1   Authentication and ciphering initiation by the network

The network initiates the authentication and ciphering procedure by transferring an AUTHENTICATION AND CIPHERING REQUEST message across the radio interface and starts timer T3360. The AUTHENTICATION AND CIPHERING REQUEST message shall contain all parameters necessary to calculate the response parameters when authentication is performed (see GSM 03.20 [13] and TS 33.102).

If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain either:

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

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

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

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

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

Additionally, the network may request the MS to include its IMEISV in the AUTHENTICATION AND CIPHERING RESPONSE message.

4.7.7.2   Authentication and ciphering response by the MS

In GSM, a 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.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION AND CIPHERING REQUEST message and perform the GSM authentication challenge. It shall not perform the authentication of the network described in 4.7.7.5.1.

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 use 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]).

4.7.7.3   Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see GSM 03.20 [13] and 3GPP TS 33.102). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent.

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

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

4.7.7.4   GPRS 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 GPRS GSM ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the GPRS UMTS ciphering key and the GPRS UMTS integrity key can be computed given the secret key associated to the IMSI.

In order to allow start of ciphering on a logical link without authentication, GPRS ciphering key sequence numbers are introduced.

The GPRS ciphering key sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the GPRS ciphering key sequence number allocated to the GPRS GSM ciphering key (in case of a GSM authentication challenge) or the GPRS UMTS ciphering key and the GPRS UMTS integrity key (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.

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

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

In UMTS, the network may choose to start ciphering and integrity checking with the stored GPRS UMTS ciphering key and the stored GPRS UMTS integrity key (under the restrictions given in GSM 02.09 and 3GPP TS 33.102) if the stored GPRS ciphering key sequence number and the one given from the MS are equal.

In GSM, the network may choose to start ciphering with the stored GPRS GSM ciphering key (under the restrictions given in GSM 02.09) if the stored GPRS ciphering key sequence number and the one given from the MS are equal and the previously negotiated ciphering algorithm is known and supported in the network. When ciphering is requested at GPRS attach, the authentication and ciphering procedure shall be performed since the MS does not store the ciphering algorithm at detach.

Upon GPRS attach, if ciphering is to be used, an AUTHENTICATION AND CIPHERING REQUEST message shall be sent to the MS to start ciphering.

If the GPRS ciphering key sequence number stored in the network does not match the GPRS ciphering key sequence number received from the MS in the ATTACH REQUEST message, then the network should authenticate the MS.

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

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

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

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

4.7.7.5   Authentication not accepted by the network

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

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

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

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

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310, T3317 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

4.7.7.5.1   Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see TS 33.102). This parameter contains two possible causes for authentication failure:

   a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a AUTHENTICATION AND CIPHERING FAILURE message to the network, with the GMM cause 'MAC failure'. 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 GMM cause 'Synch failure' and the re-synchronization token AUTS provided by the SIM (see TS 33.102). The MS shall then follow the procedure described in section 4.7.7.6 (g).

4.7.7.6   Abnormal cases on the network side

The following abnormal cases can be identified:

   a) Lower layer failure

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

   b) Expiry of timer T3360

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

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

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

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

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

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

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

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

   GPRS detach containing cause "power off":

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

   GPRS detach containing other causes than "power off":

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

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

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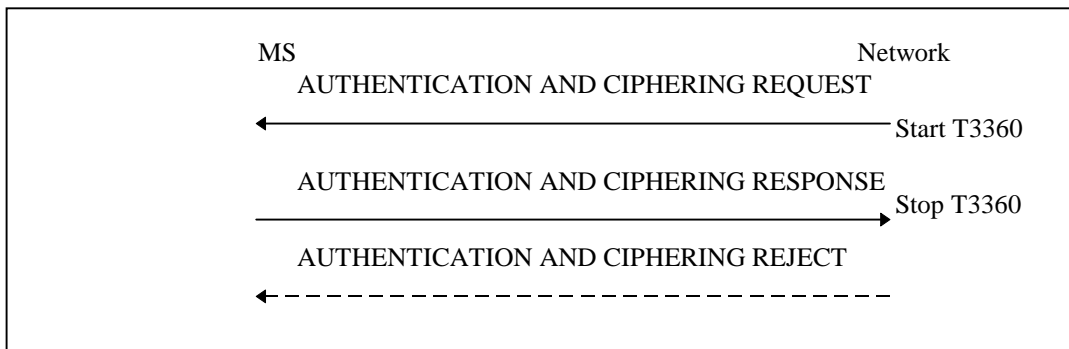

Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

(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 send the IDENTITY RESPONSE message.

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 T3318, if running, and then process the challenge information as normal.
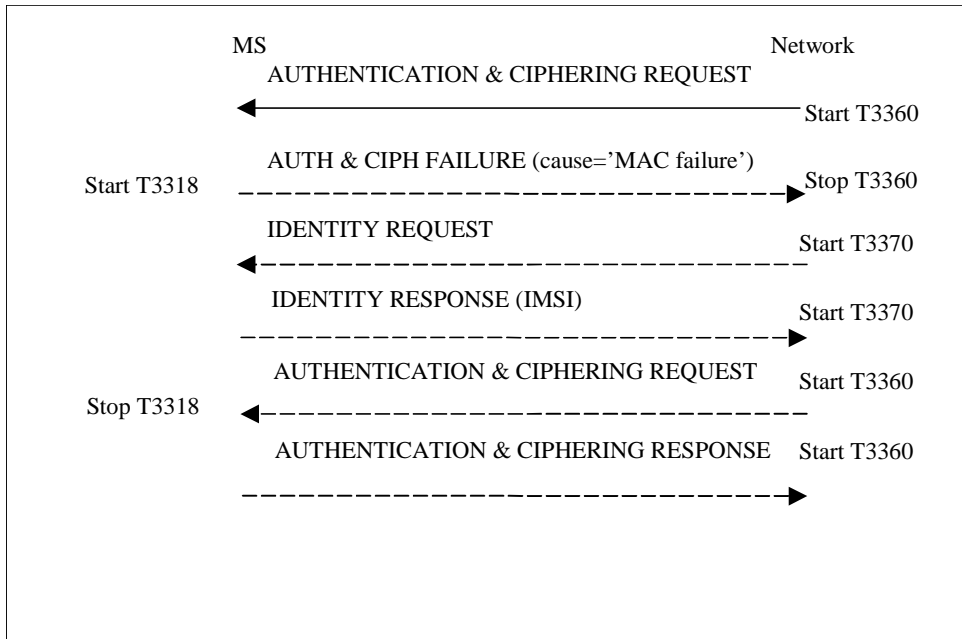
When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

Upon successfully validating the network, (an AUTHENTICATION & CIPHERING REQUEST message that contains a valid MAC is received), the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317) , if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC.

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 expires;

- Upon receipt of the second AUTHENTICATION & CIPHERING REQUEST message from the network while the T3318 is running and the MAC value 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.

Figure 4.7.7a/1 TS 24.008: Authentication failure cause 'MAC failure'

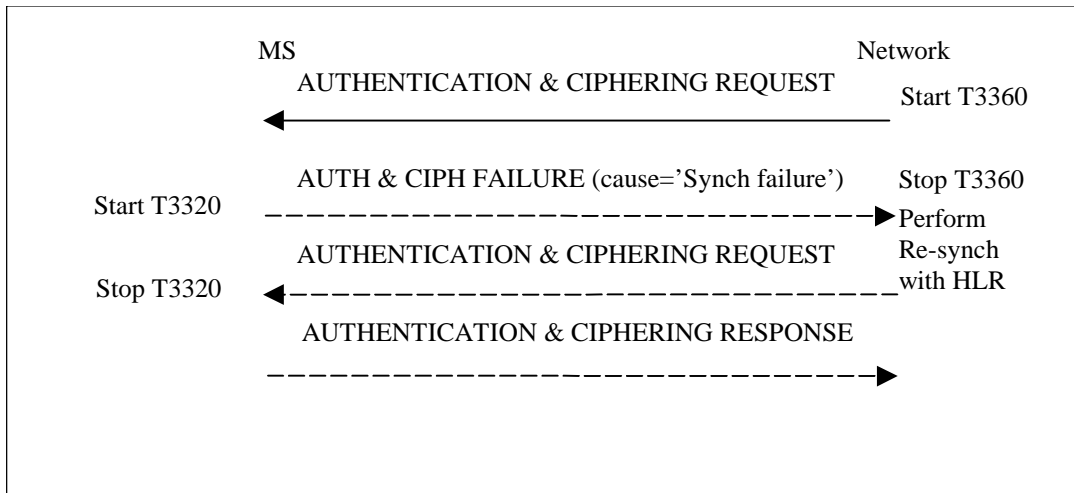(g) Authentication failure (GMM cause 'Synch failure'):

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.

When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid SQN 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, (a second AUTHENTICATION & CIPHERING REQUEST message is received which contains a valid SQN) while T3320 is running, the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid SQN.

If the MS receives a second AUTHENTICATION & CIPHERING REQUEST message which contains an invalid SQN while T3320 is running, then the MS shall behave as described in section 4.7.7.6.1.

If the timer T3320 expires, 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
              AUTHENTICATION & CIPHERING REQUEST     Re-synch
Stop T3320   ◄─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─    with HLR
              AUTHENTICATION & CIPHERING RESPONSE

             ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─►
```

Figure 4.7.7b/1 TS 24.008: Authentication failure cause 'Synch failure'

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 cell where the AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or SQN.

*** Following sections for information only ***

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	O	TLV	18

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.

The MS shall ignore the IE if it does not support UMTS authentication algorithm.

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	Authentication 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))

This IE shall not be included if MS does not support UMTS authentication algorithm.

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	O	TLV	18

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.

The MS shall ignore the IE if it does not support UMTS authentication algorithm.

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))

This IE shall not be included if MS does not support UMTS authentication algorithm.