

**21 - 24 May, 2001**

**Phoenix, USA**

---

**3GPP TSG-CN-WG1, Meeting #16**  
**26 February 2001 to 01 March 2001,**  
**Sophia France.**

***Tdoc N1-010480***

**Title:** Re-transmission of authentication requests

**Reference LS** ---  
(If available)

**Source:** [CN1]

**TO <sup>(1)</sup>:** SA3

**Cc:** ---

**WI:** Security

**Contact Person:**

**Name:** Robert Zaus  
**E-mail Address:** robert.zaus@icn.siemens.de  
**Tel. Number:** +49 170 331 5485

**Attachments:** N1-010477  
(Please list documents numbers to be attached)

**Date:** 01 March 01

---

During the last two meetings, CN1#15 and CN1#16, CN1 discussed the possibility to implement the CR 33.102-130 (S3-000725), "Re-transmission of authentication request using the same quintet", in the R'99 version of TS 24.008.

- Some delegates stated that a SIM-based solution would be more appropriate. Some delegates were also concerned that an implementation of the feature as specified by SA3 would delay the availability of standard compliant UMTS R'99 terminals.
- Other delegates were concerned that if the feature was not supported, this would greatly reduce the efficiency and grade of service of the whole system, due to a higher number of synchronisation failures and higher consumption of security quintets.

---

<sup>1</sup> Please write any action required from the groups in a clear way.

- There was a consensus that the most critical procedure for which re-transmission was expected to occur with the highest probability is the UMTS Authentication procedure via the Gb interface.

As a compromise between the points of view expressed by different delegates, CN1 agreed the change request to TS 24.008 that is attached to this liaison statement for R'99, and an identical CR for Rel-4.

CN1 hope that the agreed solution is acceptable to SA3, and kindly ask SA3 to adapt their specification TS 33.102 accordingly.

The following MM and GMM state descriptions from TS 24.008 are provided in order to help SA3 with the interpretation of the attached CR:

#### 4.1.2.1 MM sublayer states in the mobile station

....

##### 4.1.2.1.1 Main states

###### 0 NULL

The mobile station is inactive (e.g. power down). Important parameters are stored. Only manual action by the user may transfer the MM sublayer to another state.

....

###### 19. MM IDLE

There is no MM procedure running and no RR connection exists except that a local MM context may exist when the RR sublayer is in Group Receive mode. This is a compound state, and the actual behaviour of the mobile station to Connection Management requests is determined by the actual substate as described hereafter.

....

#### 4.1.3.1 GMM states in the MS

....

##### 4.1.3.1.1 Main states

###### 4.1.3.1.1.1 GMM-NULL

The GPRS capability is disabled in the MS. No GPRS mobility management function shall be performed in this state.

###### 4.1.3.1.1.2 GMM-DEREGISTERED

The GPRS capability has been enabled in the MS, but no GMM context has been established. In this state, the MS may establish a GMM context by starting the GPRS attach or combined GPRS attach procedure.

## CHANGE REQUEST

⌘ **24.008 CR CR-Num** ⌘ rev **1** ⌘ 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  Radio Access Network  Core Network

<b>Title:</b>	⌘ Re-transmission of authentication requests		
<b>Source:</b>	⌘ Siemens		
<b>Work item code:</b>	⌘ Security	<b>Date:</b>	⌘ 28 February 01
<b>Category:</b>	⌘ F	<b>Release:</b>	⌘ 99
	<p>Use <u>one</u> of the following categories:</p> <p><b>F</b> (essential correction)  <b>A</b> (corresponds to a correction in an earlier release)  <b>B</b> (Addition of feature),  <b>C</b> (Functional modification of feature)  <b>D</b> (Editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p>Use <u>one</u> of the following releases:</p> <p><b>2</b> (GSM Phase 2)  <b>R96</b> (Release 1996)  <b>R97</b> (Release 1997)  <b>R98</b> (Release 1998)  <b>R99</b> (Release 1999)  <b>REL-4</b> (Release 4)  <b>REL-5</b> (Release 5)</p>

<b>Reason for change:</b>	⌘ Currently, the stage 2 specification TS 33.102 states that if the network has to re-transmit the AUTHENTICATION REQUEST message for any reason, then it may do so using the same authentication parameters as were in the original message (RAND, AUTN). However, in the stage 3 specification TS 24.008, those parameters would be seen by the mobile as not being 'fresh' and a re-synchronisation procedure would be invoked. This would be an unnecessary use of valuable resources.
	Detection of a re-transmission is especially important in Gb mode, as according to TS 08.18 in case of a cell change the BSS may and in case of a change of the routing area it shall discard the packets queued for downlink transmission to the MS.
<b>Summary of change:</b>	⌘ For the authentication in the PS domain the MS shall remember the last received authentication parameters so that it may check whether newly received parameters are re-transmissions of previously sent parameters. For the authentication in the CS domain the same behaviour is allowed for the MS as an implementation option.
<b>Consequences if not approved:</b>	⌘ The efficiency of the system is greatly reduced, and extra signalling is carried out, due to high number of re-synchronisations

<b>Clauses affected:</b>	⌘ 4.3.2.2, 4.7.7.2, 11.2, 11.2.2		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications	⌘	
	<input type="checkbox"/> Test specifications		
	<input type="checkbox"/> O&M Specifications		
<b>Other comments:</b>	⌘ It is anticipated that SA3 will agree a CR to TS 33.102 that mandates the network to perform a Security Mode procedure after each UMTS authentication challenge.		

**How to create CRs using this form:**

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.htm). Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☒ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://www.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

## 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 ME supporting GSM or UMTS radio access.

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

### 4.3.2b Authentication Procedure used for a GSM authentication challenge

The purpose of the authentication procedure is twofold (see GSM 03.20):

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

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 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.

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 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.

A mobile station supporting UMTS authentication challenge may support the following procedure:

In order to avoid a synchronisation failure, if the same RAND is received twice, the mobile station shall store the received RAND and the RES returned from the SIM in the volatile memory and compare it with any subsequently received RAND values, until the RAND value stored in the mobile station is deleted. If the stored RAND value is equal to the new received value in the AUTHENTICATION REQUEST message, then the mobile station shall not pass the RAND to the SIM, but shall immediately send the AUTHENTICATION RESPONSE message with the stored RES. If there is no valid stored RAND in the mobile station or the stored RAND is different from the new received value in the AUTHENTICATION REQUEST message, the mobile station shall pass the RAND to the SIM, shall override any previously stored RAND and RES with the new ones and reset and restart timer T3218.

The RAND and RES values stored in the mobile station shall be deleted:

- upon receipt of a SECURITY MODE COMMAND (Iu mode only), CIPHERING MODE COMMAND (A/Gb mode only) or AUTHENTICATION REJECT message;
- upon expiry of timer T3218; or
- if the mobile station enters the MM state MM IDLE or NULL.

### 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.

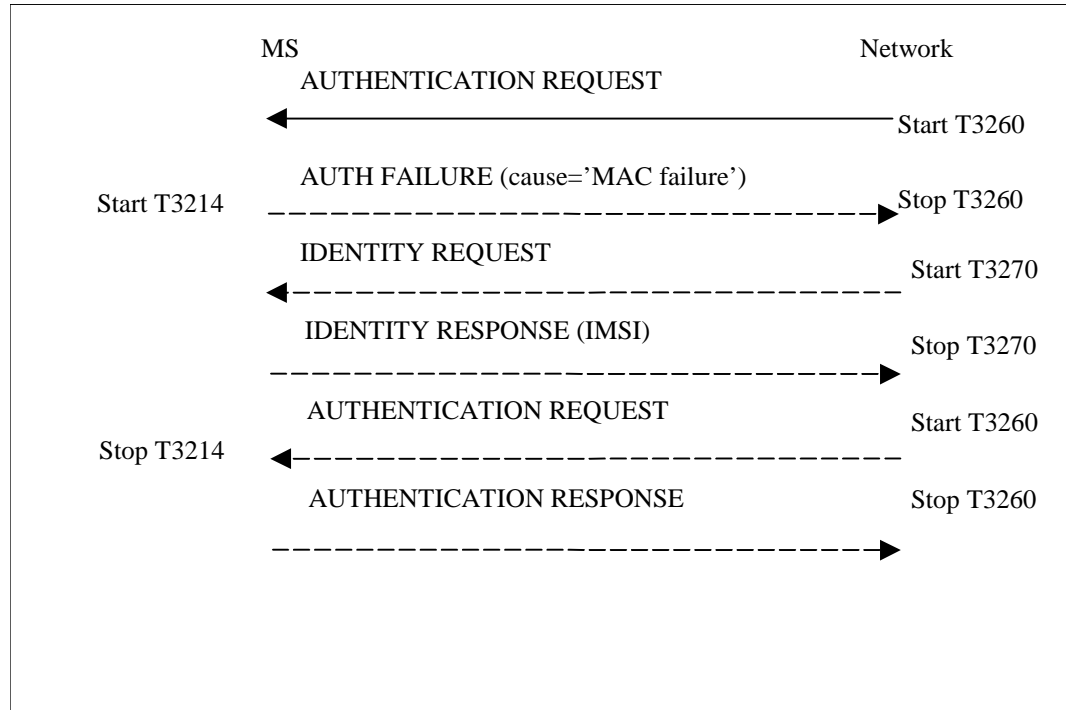
When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).

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'):

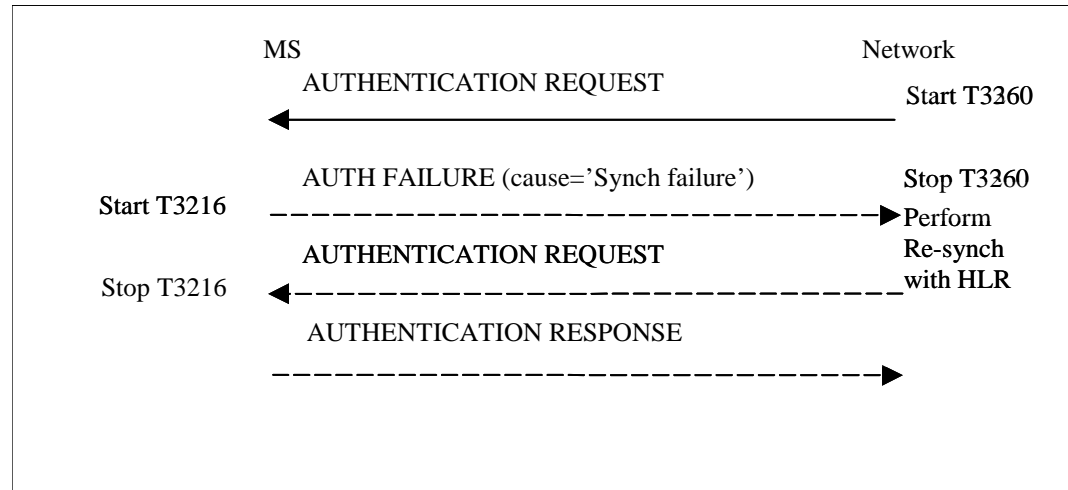
The MS shall send an AUTHENTICATION FAILURE message, with reject cause 'synch failure,' to the network and start the timer T3216. Upon receipt of an AUTHENTICATION FAILURE message from the MS with the reject cause 'synch failure,' the network shall use the returned AUTS parameter from the authentication failure parameter IE in the AUTHENTICATION FAILURE message, to re-synchronise. The re-synchronisation procedure requires the VLR/MS 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/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.

#### 4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

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

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

**Table 4.3.2.7.1/3GPP TS 24.008: Intersystem change from UMTS to GSM**

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

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

#### 4.3.2.7a Use of established security contexts

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

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be loaded from the SIM and taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in GSM 04.18 section 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named “c3” defined in 3GPP TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in 3GPP TS 33.102. The GSM ciphering key shall be loaded from the SIM and the derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in 3GPP TS 33.102.

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be loaded from the SIM and taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331).

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

#### 4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At intersystem change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

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

**Table 4.3.2.8.1/3GPP TS 24.008: Intersystem change from GSM to UMTS**

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and UMTS integrity key from the GSM cipher key provided by the SIM. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the UMTS ciphering key and the UMTS integrity key received from the UMTS security context residing in the SIM.

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

#### 4.3.2.9 Void

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

### 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 ME supporting GSM or UMTS radio access.

The authentication and ciphering procedure can be used for either:

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

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

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

#### 4.7.7b Authentication and ciphering procedure used for GSM authentication challenge

The purpose of the authentication and ciphering procedure is threefold (see GSM 03.20 [13]):

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

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]).

A mobile station supporting UMTS authentication challenge shall support the following procedure:

In order to avoid a synchronisation failure, if the same RAND is received twice, the mobile station shall store the received RAND and the RES returned from the SIM in the volatile memory and compare it with any subsequently received RAND values, until the RAND value stored in the mobile station is deleted. If the stored RAND value is equal to the new received value in the AUTHENTICATION & CIPHERING REQUEST message, then the mobile station shall not pass the RAND to the SIM, but shall immediately send the AUTHENTICATION & CIPHERING RESPONSE message with the stored RES. If there is no valid stored RAND in the mobile station or the stored RAND is different from the new received value in the AUTHENTICATION & CIPHERING REQUEST message, the mobile station shall pass the RAND to the SIM, shall override any previously stored RAND and RES with the new ones and reset and restart timer T3316.

The RAND and RES values stored in the mobile station shall be deleted:

- upon receipt of a SECURITY MODE COMMAND (Iu mode only) or AUTHENTICATION & CIPHERING REJECT message;
- upon expiry of timer T3316; or
- if the mobile station enters the GMM states GMM-DEREGISTERED or GMM-NULL.

#### 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":

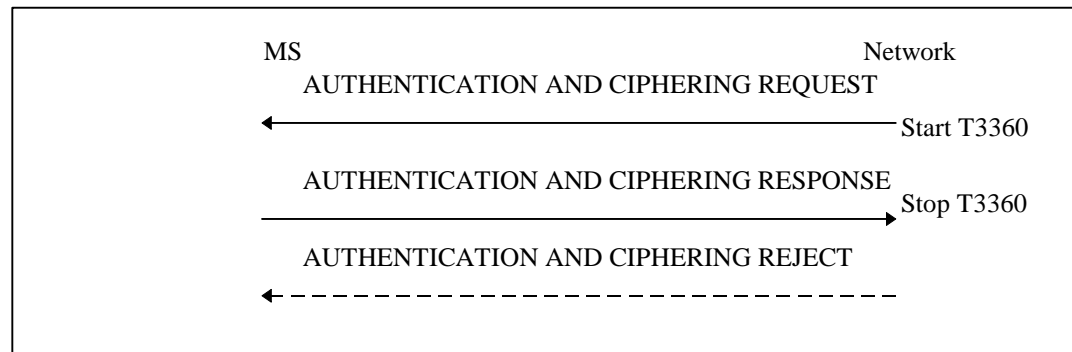
If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall abort the authentication and ciphering procedure and shall progress the GPRS detach procedure.

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.



**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.

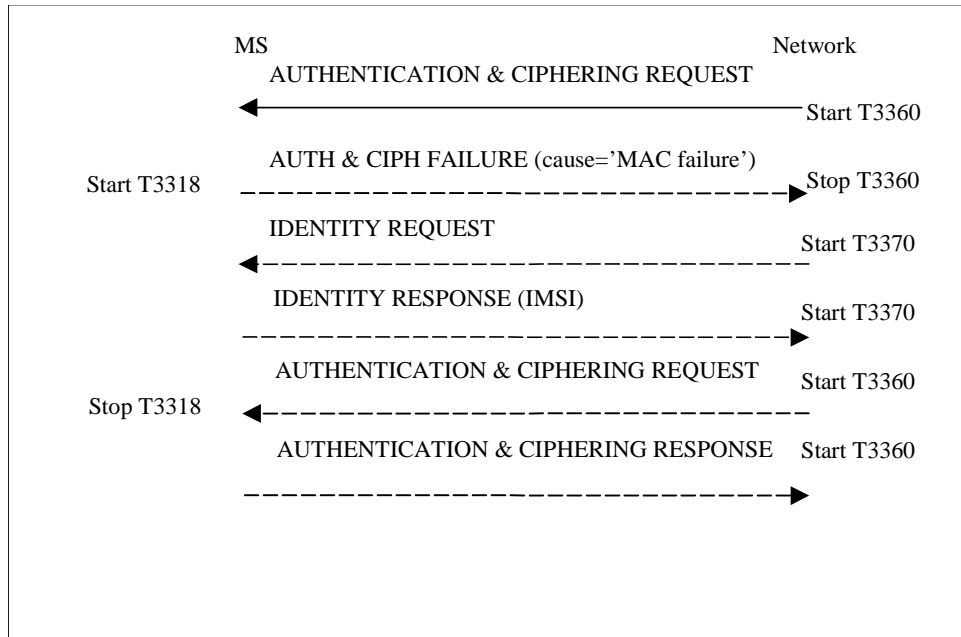
When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

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.

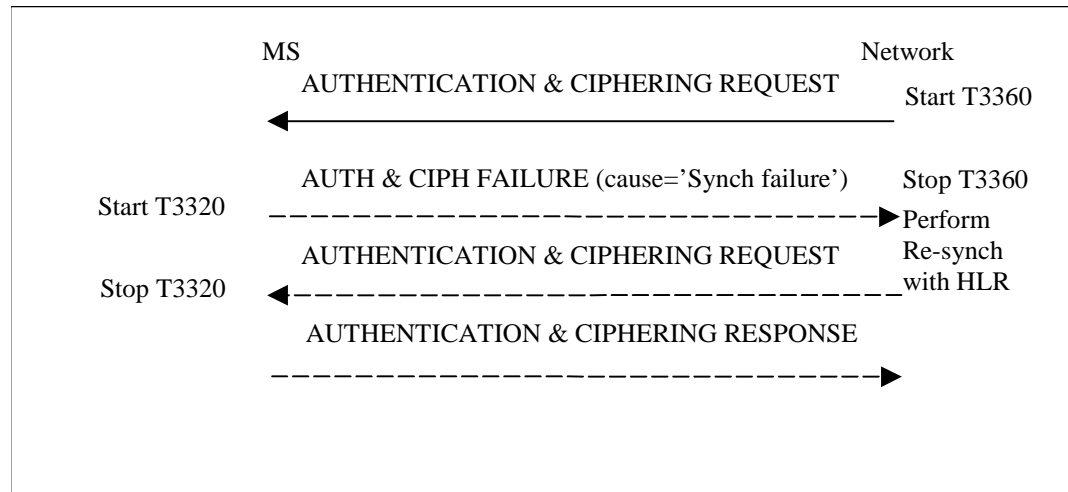
When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid SQN has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

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.



**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.

#### 4.7.7.7 Use of established security contexts

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

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in 3GPP TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102.

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331).

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

#### 4.7.7.8 Handling of keys at intersystem change from UMTS to GSM

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

The ME shall handle the GPRS GSM ciphering key according to Table 4.7.7.8.1.

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

**Table 4.7.7.8.1/3GPP TS 24.008: Intersystem change from UMTS to GSM**

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

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

#### 4.7.7.9 Handling of keys at intersystem change from GSM to UMTS

At an intersystem change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to Table 4.7.7.9.1.

**Table 4.7.7.9.1/3GPP TS 24.008: Intersystem change from GSM to UMTS**

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and GPRS UMTS integrity key from the GPRS GSM cipher key provided by the SIM. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the GPRS UMTS ciphering key and the GPRS UMTS integrity key received from the UMTS security context residing in the SIM.

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

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



## 11.2 Timers of mobility management

Table 11.1/3GPP TS 24.008: Mobility management timers - MS-side

TIMER NUM.	MM ST AT	TIME OUT VAL.	CAUSE FOR START	NORMAL STOP	AT THE EXPIRY
T3210	3	20s	- LOC_UPD_REQ sent	- LOC_UPD_ACC - LOC_UPD_REJ - AUTH_REJ - Lower layer failure	Start T3211
T3211	1 2	15s	- LOC_UPD_REJ with cause#17 netw. failure - lower layer failure or RR conn. released after RR conn. abort during loc. updating	- Time out - cell change - request for MM connection establishment - change of LA	Restart the Location update proc.
T3212	1, 2	Note 1	- termination of MM service or MM signalling	- initiation of MM service or MM signalling	initiate periodic updating
T3213	1 2 11	4s	- location updating failure	- expiry - change of BCCH parameter	new random attempt
T3214	3 5 7	20s	AUTHENT FAILURE Cause = MAC failure sent	AUTHENT REQ - received	Consider the network as 'false' (see 4.3.2.6.1)
T3216	3 5 7	15s	AUTHENT FAILURE Cause = Synch failure sent	AUTHENT REQ received	Consider the network as 'false' (see 4.3.2.6.1)
<u>T3218</u>	<u>3</u> <u>5</u> <u>7</u>	<u>20s</u>	<u>RAND and RES stored after receipt of a UMTS authentication challenge</u>	- <u>Cipher mode setting (A/Gb mode only)</u> - <u>Security mode setting (lu mode only)</u> - <u>AUTHENT REJ received</u> - <u>enter MM IDLE or NULL</u>	<u>Delete the stored RAND and RES</u>

T3220	7	5s	- IMSI DETACH	- release from RM-sublayer	enter Null or Idle, ATTEMPTING TO UPDATE
T3230	5	15s	- CM SERV REQ CM REEST REQ	- Cipher mode setting - CM SERV REJ - CM SERV ACC	provide release ind.
T3240	9 10	10s	see section 11.2.1	see section 11.2.1	abort the RR connection

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

**Table 11.2/3GPP TS 24.008: Mobility management timers - network-side**

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

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

## 11.2.1 Timer T3240

Timer T3240 is started in the mobile station when:

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

Timer T3240 is stopped, reset, and started again at receipt of an MM message.

Timer T3240 is stopped and reset (but not started) at receipt of a CM message that initiates establishment of an CM connection (an appropriate SETUP, REGISTER, or CP-DATA message as defined in 3GPP TS 24.008, 3GPP TS 24.010 or GSM 04.11).

## 11.2.2 Timers of GPRS mobility management

**Table 11.3/3GPP TS 24.008: GPRS Mobility management timers - MS side**

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1 <sup>st</sup> , 2 <sup>nd</sup> , 3 <sup>rd</sup> , 4 <sup>th</sup> EXPIRY Note 3
T3310	15s	GMM-REG-INIT	ATTACH REQ sent	ATTACH ACCEPT received ATTACH REJECT received	Retransmission of ATTACH REQ
T3311	15s	GMM-DEREG ATTEMPTING TO ATTACH or GMM-REG ATTEMPTING TO UPDATE	ATTACH REJ with other cause values as described in chapter 'GPRS Attach' ROUTING AREA UPDATE REJ with other cause values as described in chapter 'Routing Area Update' Low layer failure	Change of the routing area	Restart of the Attach or the RAU procedure with updating of the relevant attempt counter
T3316	30s	<u>GMM-REG-INIT</u> <u>GMM-REG</u> <u>GMM-DEREG-INIT</u> <u>GMM-RA-UPDATING-INT</u> <u>GMM-SERV-REQ-INIT</u> (lu mode only)	<u>RAND and RES stored after receipt of a UMTS authentication challenge</u>	<u>Security mode setting</u> (lu mode only)  <u>AUTHENTICATION &amp; CIPHERING REJECT received</u>  <u>Enter GMM-DEREG or GMM-NULL</u>	<u>Delete the stored RAND and RES</u>

T3318	20s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=MAC failure) sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
T3320	15s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=synch failure) sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
T3321	15s	GMM-DEREG-INIT	DETACH REQ sent	DETACH ACCEPT received	Retransmission of the DETACH REQ
T3330	15s	GMM-ROUTING-UPDATING-INITIATED	ROUTING AREA UPDATE REQUEST sent	ROUTING AREA UPDATE ACC received  ROUTING AREA UPDATE REJ received	Retransmission of the ROUTING AREA UPDATE REQUEST message

**Table 11.3a/3GPP TS 24.008: GPRS Mobility management timers – MS side**

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3302	Default 12 min Note 1	GMM-DEREG or GMM-REG	At attach failure and the attempt counter is greater than or equal to 5. At routing area updating failure and the attempt counter is greater than or equal to 5.	At successful attach  At successful routing area updating	On every expiry, initiation of the GPRS attach procedure or RAU procedure
T3312	Default 54 min Note1	GMM-REG	In GSM, when READY state is left. In UMTS, when PMM-CONNECTED mode is left.	When entering state GMM-DEREG	Initiation of the Periodic RAU procedure
T3314 READY (GSM only)	Default 44 sec Note 2	All except GMM-DEREG	Transmission of a PTP PDU	Forced to Standby	No cell-updates are performed
T3317 (UMTS only)	10s	GMM-SERVICE-REQUEST-INITIATED	SERVICE REQ sent	Security mode control procedure is completed, SERVICE ACCEPT received, or SERVICE REJECT received	Abort the procedure

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

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

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

**Table 11.4/3GPP TS 24.008: GPRS Mobility management timers - network side**

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

**Table 11.4a/3GPP TS 24.008: GPRS Mobility management timers - network side**

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

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

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

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