3GPP TSG_CN **Tdoc NP-000445**
Plenary Meeting #9, Oahu, Hawaii
20th – 22nd September 2000.

Source: **TSG_N WG 1**

Title: **CRs to R99 Work Item Security**

Agenda item: **8.3.1**

Document for: **APPROVAL**

Introduction:

This document contains 3 CRs on R99 Work Item Security, that has been agreed by TSG_N WG1, and is forwarded to TSG_N Plenary meeting #9 for approval.

Spec	CR	R	Doc-2nd-Level	Phase	Subject	Cat	Ver_C	Ver_N
24.008	261		N1-000993	R99	Correction of the storage of the ciphering key	F	3.4.1	3.5.0
24.008	252		N1-000948	R99	Modifications to the authentication failure procedure	F	3.4.1	3.5.0
24.008	230	1	N1-000996	R99	Network Authentication Failure	F	3.4.1	3.5.0

3GPP-CN1 Meeting #13
Vancouver/Canada, 14-18 August 2000

***Document* N1-000948**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

24.008	CR	252	Current Version:	3.4.1

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

For submission to:	TSG CN#9	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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

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

Source: TSGN1 **Date:** 10/08/00

Subject: Modifications to the authentication failure procedure

Work item: Security

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

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

Reason for change: In GPRS, where the MS has a UMTS security context and receives an AUTHENTICATION & CIPHERING REQUEST containing an invalid MAC in cell A, the MS sends an AUTHENTICATION & CIPHERING FAILURE message to the network (on cell A) and starts the timer T3318. If the mobile then moves to cell B and performs the cell update procedure and T3318 expires, then the MS needs to treat the cell where it received the AUTHENTICATION & CIPHERING REQUEST as barred (cell A), and should not treat the new cell (cell B) as barred. The circuit switched side is not affected, because there is no cell update procedure, but this CR clarifies the wording anyway.

Clauses affected: 4.3.2.6.1, 4.3.2.7, 4.7.7.6.1

Other specs affected:

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

Other comments: This CR also corrects a formatting mistake.

help.doc

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

*** First modified sub-clause ***

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

If the MS deems that the network has failed the authentication check, then the it shall treat the ~~current serving~~ cell where the ~~authentication failure occurred~~AUTHENTICATION REQUEST message was received as barred, until refresh of system information data~~4.3.2.7 Handling of keys at intersystem change from UMTS to GSM~~

*** Next modified sub-clause ***

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

*** Last modified sub-clause ***

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

If the MS deems that the network has failed the authentication check, then it shall treat the ~~current serving~~ cell where the ~~authentication failure occurred~~AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data.

3GPP-CN1/SMG3WPA Meeting #13
Vancouver/Canada, 14-18 August 2000

***Document* N1-000993**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

24.008	CR	261	Current Version:	3.4.1

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

For submission to:	CN#9	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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

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

Source: TSGN1 **Date:** 15.08.2000

Subject: Correction of the storage of the ciphering key

Work item: Security

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

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

Reason for change: During the introduction of the UMTS security procedures, the point in time when the ME is required to load the ciphering key (and the integrity key) from the SIM and store it the ME was changed unintentionally. This CR proposes to restore the original behaviour. - This does not prevent different implementations with the ME storing the new ciphering key already at an earlier point in time.

Clauses affected: 4.3.2.2, 4.3.2.7a

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

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

4.3.2.2 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~~, a UMTS ciphering key, a UMTS integrity key~~ to the ME. A GSM authentication challenge will result in the SIM passing an SRES ~~and a GSM ciphering key~~ to the ME.

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

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 TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in TS 33.102. The 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 TS 25.331). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in TS 33.102.

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be 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 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.

********** ANNEX: quotation from GSM 04.08, v 7.7.0 **********

4.3.2.2 Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. It shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network. The new ciphering key calculated from the challenge information shall overwrite the previous one and be stored on the SIM before the AUTHENTICATION RESPONSE message is transmitted. **The ciphering key stored in the SIM shall be loaded in to 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 section 3.4.7.2). The ciphering

3GPP/SMG Meeting #13
Vancouver, Canada, 14 – 18 August 2000

Document N1-000996
Rev of N1-000887

CHANGE REQUEST

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

24.008 **CR** **230r1** Current Version: 3.4.1

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

For submission to: CN #9 *list expected approval meeting # here ↑*

for approval [X] for information [ ]

strategic [ ] non-strategic [ ] *(for SMG use only)*

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

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

Source: TSGN1 **Date:** 2000-08-15

Subject: Network authentication failure

Work item: Security

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

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

Reason for change:

This CR proposes to simplify the procedures in the MS when an authentication failure with MAC failure has occurred, by proposing to use one timer (T3214 for CS services or T3318 for PS services) instead of two timers (T3214 and T3215 for CS services or T3318 and T3319 for PS services).

The suspend/resume of the retransmission timers during the authentication procedure need to be clarified. Instead of suspending and resuming the retransmission timers it should be possible for the MS to stop and restart the timers with the initial value.

Furthermore, the description of the MS behaviour when receiving an Authentication Request or Authentication and Ciphering Request with 'Synch failure' is not complete.

Clauses affected: 4.3.2.6, 4.7.7.6, 11.2, 11.2.2

Other specs Affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

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 MAC failure case, the procedural behaviour is ffs.~~ In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

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 parameters 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 ~~stop timer T3214 if running and then~~ send the IDENTITY RESPONSE message. ~~At the sending of this message, the MS shall start the timer T3215.~~

If the TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the MS. Upon receiving the second AUTHENTICATION

REQUEST message from the network, the MS shall stop the timer T3214~~5~~, 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~~s~~ a valid MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start ~~resume~~ 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 ~~that are currently suspended if they are not not already running~~.

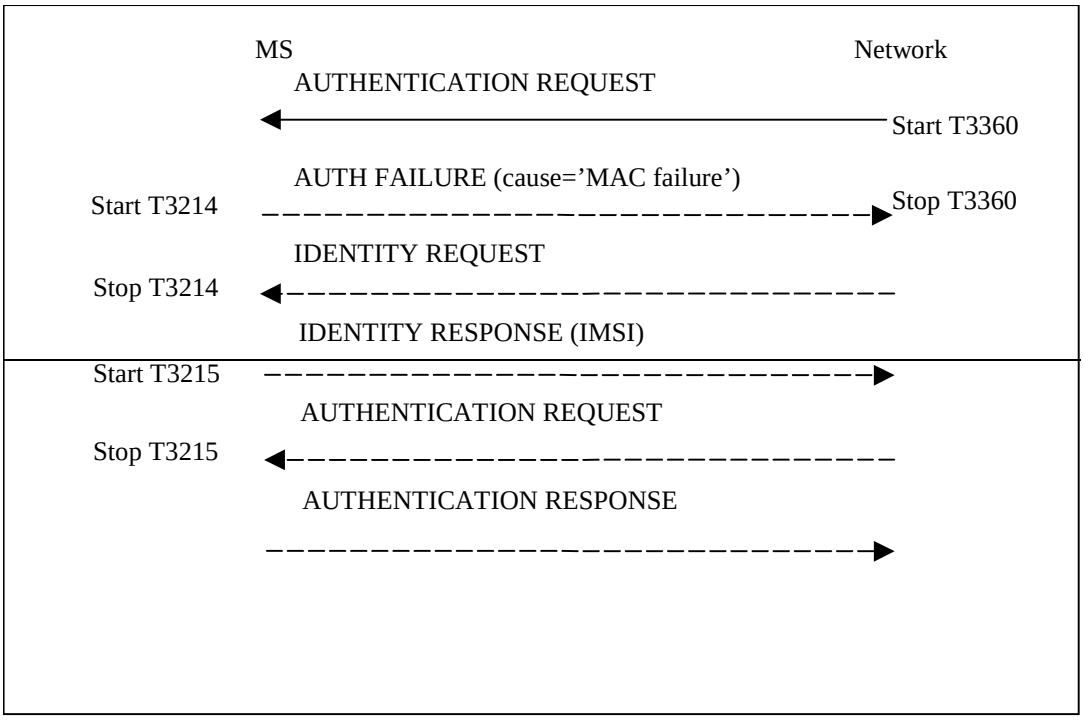
It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occur:

- After sending the AUTHENTICATION FAILURE message with the reject cause 'MAC failure' the timer T3214 expires~~times out~~;

~~- After sending the IDENTITY RESPONSE message the timer T3215 times out; or~~

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

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



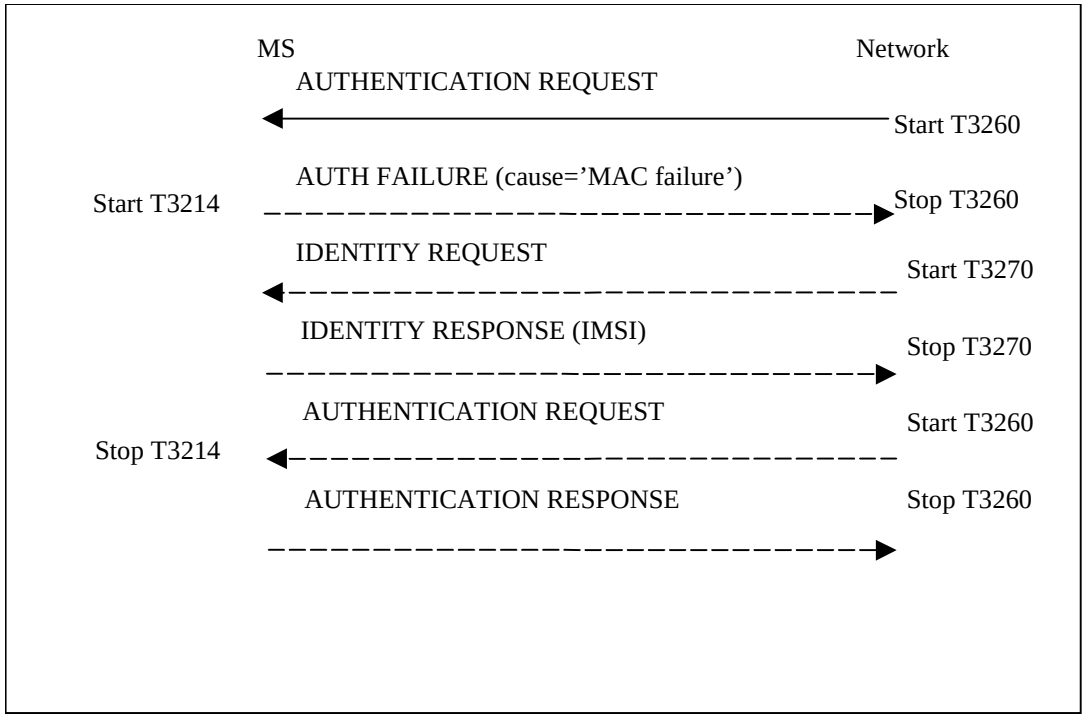


Figure 4.2/TS 24.008: Authentication Failure Procedure (reject cause 'MAC failure')

(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 ~~second~~ 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~~times out~~, then the MS shall behave as described in section 4.3.2.6.1.

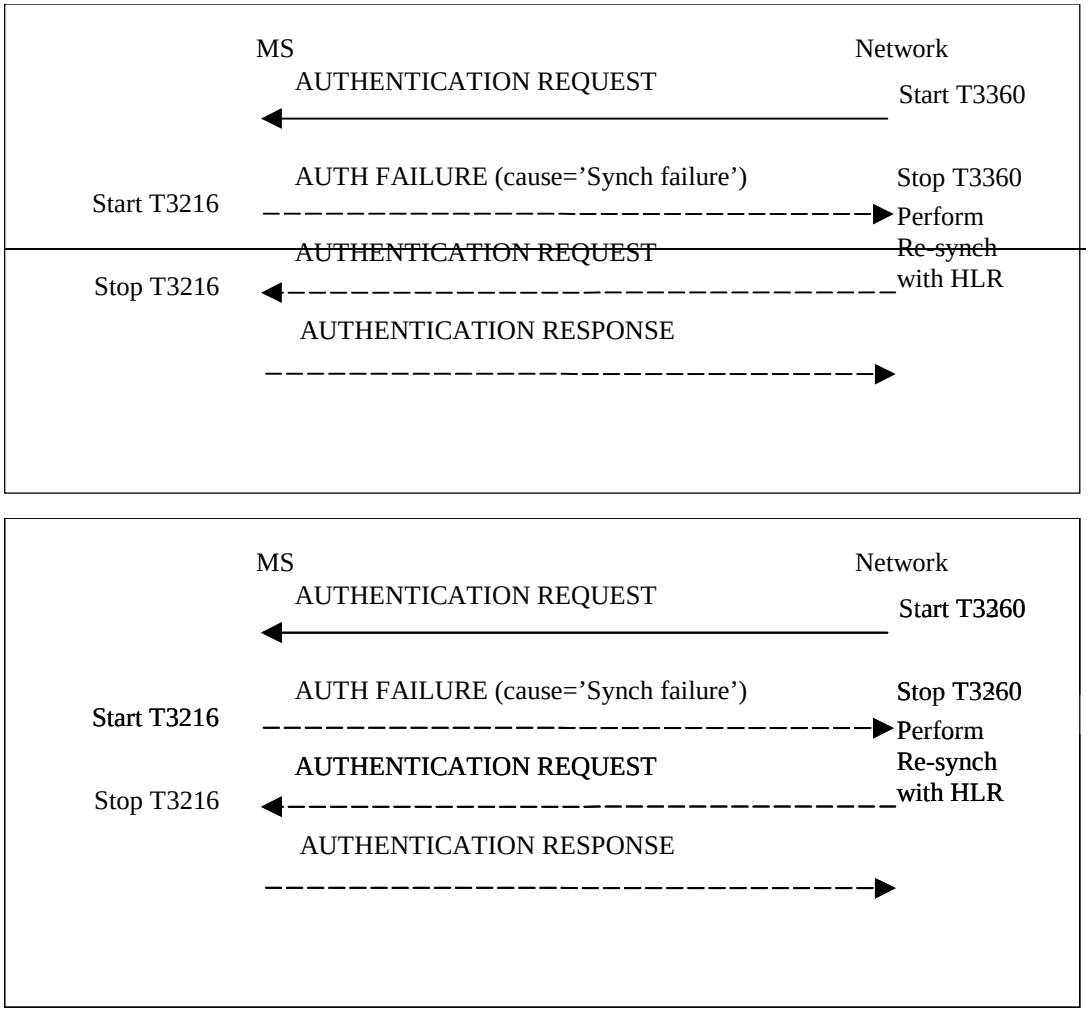


Figure 4.2a/TS 24.008: Authentication Failure Procedure (reject cause 'Synch failure')

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 current serving cell where the authentication failure occurred 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.

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

4.7.7.3 Authentication and ciphering completion by the network

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

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

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

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.

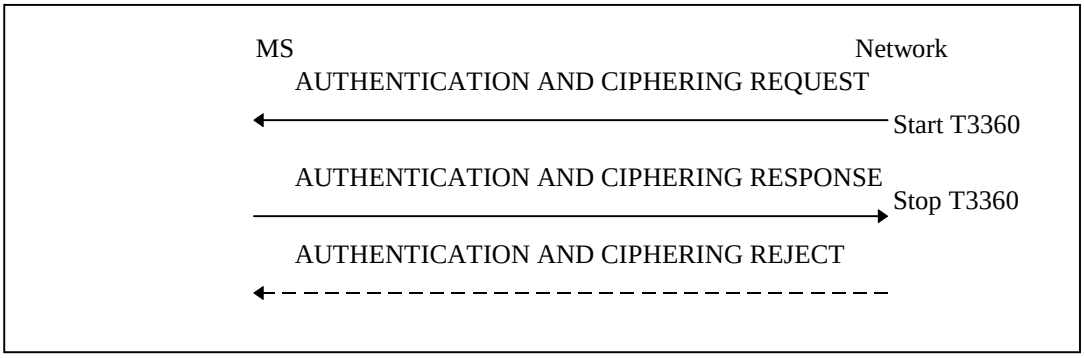


Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

(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 ~~stop timer T3318, if running, and then~~ send the IDENTITY RESPONSE message. ~~At the sending of this message, the MS shall start the timer T3319.~~

If the P-TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION & CIPHERING REQUEST message to the MS. Upon receiving the second AUTHENTICATION & CIPHERING REQUEST message from the network, the MS shall stop timer T3318~~9~~, 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~~ing~~ a valid MAC is received), the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start ~~resume~~ 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 ~~that are currently suspended, if they are not already running~~.

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

- After sending the AUTHENTICATION & CIPHERING FAILURE message with GMM cause 'MAC failure' the timer T3318 expires~~times out~~;

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

- Upon receipt of the second AUTHENTICATION & CIPHERING REQUEST message from the network~~,~~ while the T3318 is running and the MAC value ~~still~~ cannot be resolved.

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

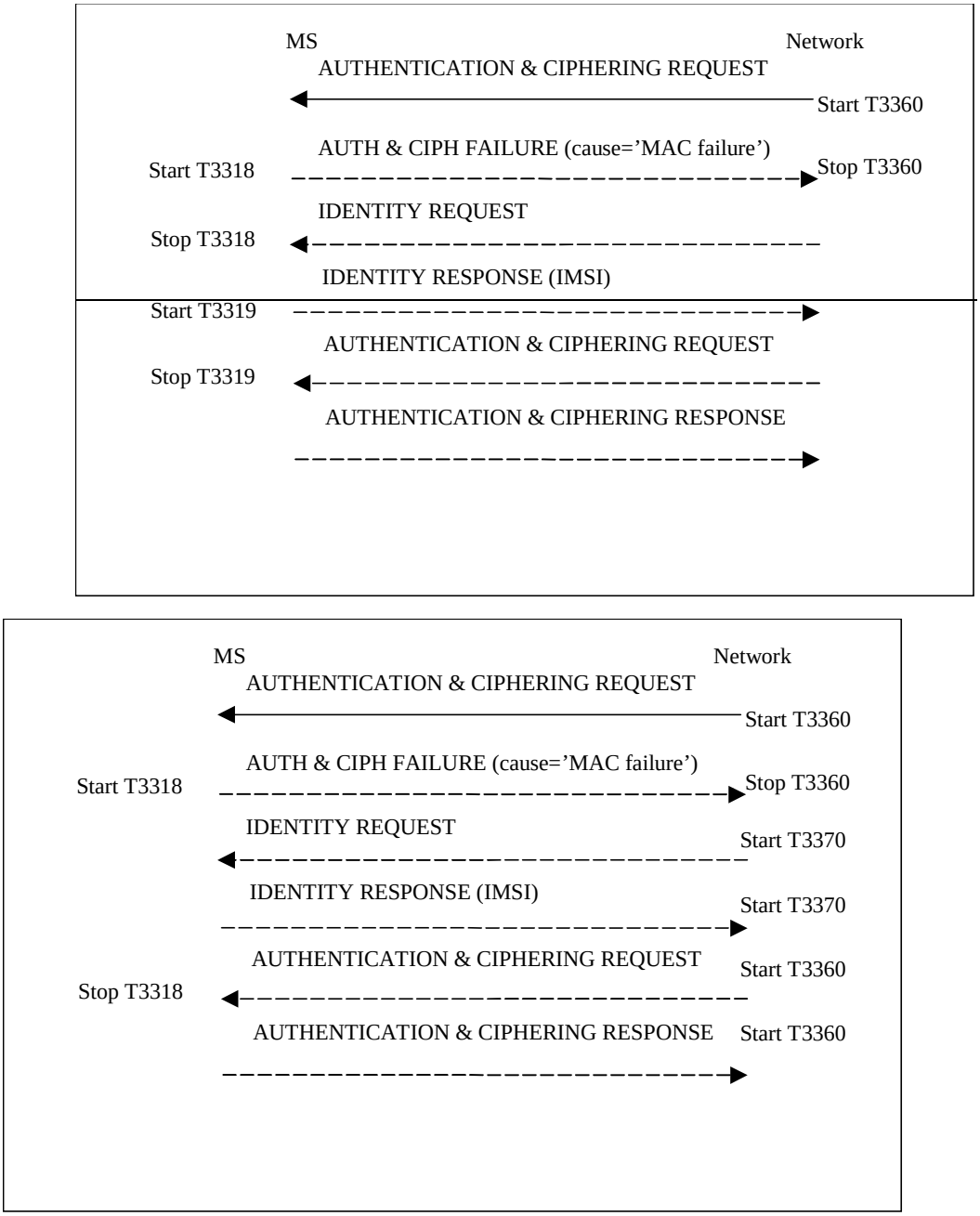


Figure 4.7.7a/1 TS 24.008: Authentication failure cause 'MAC failure'

(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~~times out~~, the MS shall behave as described in section 4.7.7.6.1.

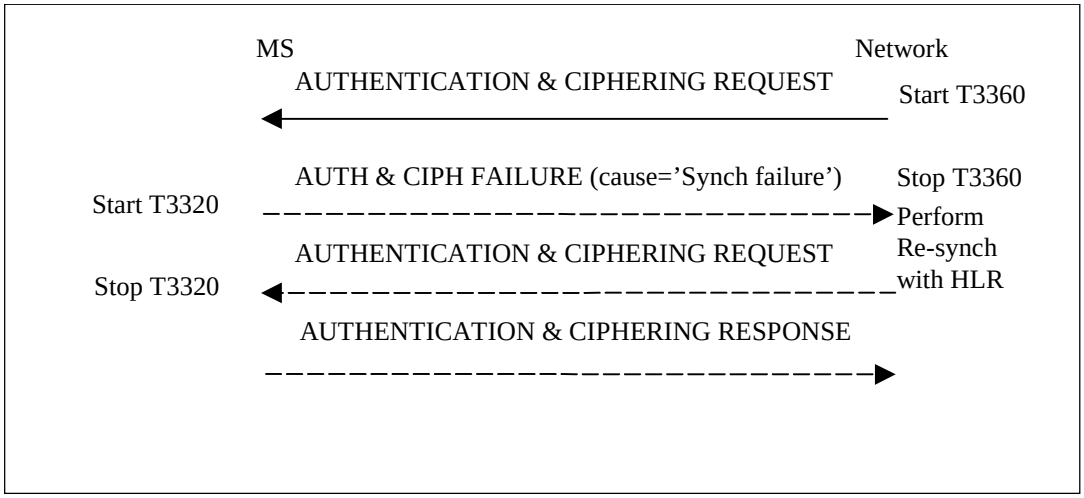


Figure 4.7.7b/1 TS 24.008: Authentication failure cause 'Synch failure'

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 current serving cell where the authentication failure occurred 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.

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

11.2 Timers of mobility management

Table 11.1/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	~~5~~20s	AUTHENT FAILURE Cause = MAC failure sent	~~ID REQUEST received~~ - AUTHENT REQ - received	Consider the network as 'false' (see 4.3.2.6.1)
~~T3215~~	~~3~~ ~~5~~ ~~7~~	~~15s~~	~~ID RESPONSE sent~~	~~AUTHENT REQ received~~	~~Consider the network as 'false' (see 4.3.2.6.1)~~
T3216~~5~~	3 5 7	15s	AUTHENT FAILURE Cause = Synch failure sent	AUTHENT REQ received	Consider the network as 'false' (see 4.3.2.6.1)
T3220	7	5s	- IMSI DETACH	- release from RM-sublayer	enter Null or Idle, ATTEMPTING TO UPDATE
T3230	5	15s	- CM SERV REQ CM REEST REQ	- Cipher mode setting - CM SERV REJ - CM SERV ACC	provide release ind.
T3240	9 10	10s	see section 11.2.1	see section 11.2.1	abort the RR connection

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

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

TIMER NUM.	MM 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 ~~Procedural behavior is FFS~~	
T3270	4	12s	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Optionally Release RR connection	

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

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

11.2.2 Timers of GPRS mobility management

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

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st , 2nd, 3rd , 4th EXPIRY Note 3
T3310	15s	GMM-REG-INIT	ATTACH REQ sent	ATTACH ACCEPT received ATTACH REJECT received	Retransmission of ATTACH REQ
T3311	15s	GMM-DEREG ATTEMPTING TO ATTACH or GMM-REG ATTEMPTING TO UPDATE	ATTACH REJ with other cause values as described in chapter 'GPRS Attach' ROUTING AREA UPDATE REJ with other cause values as described in chapter 'Routing Area Update' Low layer failure	Change of the routing area	Restart of the Attach or the RAU procedure with updating of the relevant attempt counter
T3318	~~5~~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	~~IDENTITY REQUEST~~ AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
~~T3319~~	~~15s~~	~~GMM-REG-INIT~~ ~~GMM-REG~~ ~~GMM-DEREG-INIT~~ ~~GMM-RA-UPDATING-INT~~ ~~GMM-SERV-REQ-INIT (UMTS only)~~	~~IDENTITY RESPONSE sent~~	~~AUTHENTICATION & CIPHERING REQUEST received~~	~~On first expiry, the MS should consider the network as false (see 4.7.7.6.1)~~
T3320	15s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=synch failure) sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)
T3321	15s	GMM-DEREG-INIT	DETACH REQ sent	DETACH ACCEPT received	Retransmission of the DETACH REQ
T3330	15s	GMM-ROUTING-UPDATING-INITIATED	ROUTING AREA UPDATE REQUEST sent	ROUTING AREA UPDATE ACC received ROUTING AREA UPDATE REJ received	Retransmission of the ROUTING AREA UPDATE REQUEST message

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

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

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

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

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

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

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

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

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

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

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

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