3GPP TSG CN Plenary
Meeting #10, Bangkok, Thailand
6th – 8th December 2000

Tdoc NP-000672

Source: **TSG CN WG 1**

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

Agenda item: **7.3**

Document for: **APPROVAL**

Introduction:

This document contains 4 CRs on **R99** Work Item **”Security”**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #10 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
24.008	308		N1-001285	R99	Correction of the timer list	F	3.5.0
24.008	318		N1-001396	Rel-4	Correction of the timer list	A	4.0.0
24.008	289	2	N1-001419	R99	The application of security procedures to	F	3.5.0
24.008	290	2	N1-001420	Rel-4	The application of security procedures to	A	4.0.0

3GPP TSG-CN1 Meeting #14
Cardiff, Wales - 20 - 24 November, 2000

Tdoc N1-001285

CR-Form-v3

CHANGE REQUEST

⌘	**24.008**	**CR**	**308**	⌘	rev	**-**	⌘	Current version:	**3.5.0**	⌘	

*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 □

Title:	⌘	Correction of the timer list		
Source:	⌘	Fujitsu, NTT Software		
Work item code:	⌘	Security	***Date:*** ⌘	16/Nov/2000
Category:	⌘	**F** Critical correction	***Release:*** ⌘	R99

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The timer T3317, which is set to the MS to wait the Service Accept message, shall be stoped if the Service Request procedure is running when MS receives Authentication and Ciphering Reject message.
Summary of change:	⌘	The timer T3317 is stopped when the Authentication and Ciphering Reject message is received by the MS.
Consequences if not approved:	⌘	The timer T3317 will be still running.

Clauses affected:	⌘	4.7.7.5	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

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. 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.

4.7.7.5 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.

3GPP TSG-CN1 Meeting #14
Cardiff, Wales - 20 - 24 November, 2000

Tdoc N1-001396

CR-Form-v3

CHANGE REQUEST

⌘	**24.008**	**CR**	**318**	⌘	rev	**-**	⌘	Current version:	**4.0.0** ⌘

*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 □

Title: ⌘	Correction of the timer list			
Source: ⌘	Fujitsu, NTT Software			
Work item code: ⌘	Security		***Date:*** ⌘	23/Nov/2000
Category: ⌘	**A** Critical correction		***Release:*** ⌘	REL-4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘	The timer T3317, which is set to the MS to wait the Service Accept message, shall be stoped if the Service Request procedure is running when MS receives Authentication and Ciphering Reject message.
Summary of change: ⌘	The timer T3317 is stopped when the Authentication and Ciphering Reject message is received by the MS.
Consequences if not approved: ⌘	The timer T3317 will be still running.

Clauses affected: ⌘	4.7.7.5	
Other specs affected: ⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments: ⌘		

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. 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.

4.7.7.5 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.

3GPP TSG-CN1 Meeting #14 ***Tdoc N1-00~~1335~~1419***

revised N1-001262

Cardiff, Wales - 20 - 24 November, 2000

CR-Form-v3

CHANGE REQUEST

⌘	**24.008**	**CR**	**289**	⌘	rev	**r~~1~~2**	⌘	Current version: **3.5.0** ⌘

*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 ☒

Title:	⌘	Application of security procedures to emergency calls		
Source:	⌘	Vodafone, Siemens		
Work item code:	⌘	Security	***Date:*** ⌘	08-11-2000
Category:	⌘	F	***Release:*** ⌘	R99

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘ Following a CR against 33.102, sent for information by SA3 (in document N1-000991) it was noted that the stage two requirements for applying the security features to emergency calls have changed in such a way as to be mis-aligned with the stage three specifications in 24.008. The stage two requirements, in 33.102, now read:

6.4.9 Emergency call handling

PLMNs shall support an emergency call teleservice as defined in TS 22.003 which fulfils the additional service requirements defined in TS 22.101.

6.4.9.1 Security procedures applied

The security mode procedure shall be applied as part of emergency call establishment as defined in TS 24.008. Thus, integrity protection (and optionally ciphering) shall be applied as for a non-emergency call. If authentication of the (U)SIM fails for any reason, the emergency call shall proceed as in 6.4.9.2 d) below. Once the call is in progress with integrity protection (and optionally ciphering) applied, failure of integrity checking or ciphering is an unusual circumstance and must be treated in the same manner as other equipment failures, that is, the call will terminate.

6.4.9.2 Security procedures not applied

As a serving network option, emergency calls may be established without the network having to apply the security mode procedure as defined in TS 24.008.

The following are the only cases where the "security procedure not applied"

		option may be used : a) Authentication is impossible because the (U)SIM is absent b) Authentication is impossible because the serving network cannot obtain authentication vectors due to a network failure c) Authentication is impossible because the (U)SIM is not permitted to receive non-emergency services from the serving network (e.g. there is no roaming agreement or the IMSI is barred) d) Authentication is possible but the serving network cannot successfully authenticate the (U)SIM This CR aims to bring 24.008 into line with what is specified above.
Summary of change:	⌘	The Mobile Station must be ready to continue the signalling for an emergency call with or without the security procedures having been applied. The MSC will make the decision as to whether or not security is applied to the emergency call.
Consequences if not approved:	⌘	Mobiles will be manufactured in such a way that network operators and users may have to compromise their level of security.

Clauses affected:	⌘	4.1.1.1.1, 4.1.1.1.1a, 4.5.1		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘	An identical change to 24.008 v4.0.0 exists in N1-001336		

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. 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.

*** First Modified Sub-Clause ***

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

In UMTS only, integrity protected signalling is mandatory with one exception regarding emergency calls (see 4.1.1.1.1a). In UMTS only, all layer 3 protocols shall use integrity protected signalling once the security mode procedure has been successfully activated in the network and the MS. Integrity protection of all layer 3 signalling messages is the responsibility of lower layers. It is the network which activates integrity protection. This is done using the security mode control procedure (TS 25.331).

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

The CS and PS domains in the network and the MM and GMM layers in the MS, are not aware of whether integrity protection has been started in the lower layers by the other domain. It is mandatory for the network to initiate one security mode control procedure for the CS domain and one for the PS domain.

~~Not all MM/GMM messages are integrity protected. Therefore, the following MM/GMM messages shall be accepted by the MM and GMM entities of the MS if they are received, before the security mode control procedure for that domain is activated in the lower layers in the MS:~~

Except the messages listed below, no layer 3 ~~NAS~~ signalling messages shall be processed by the receiving MM and GMM entities or forwarded to the CM entities, unless the security mode control procedure is activated for that domain.

- MM messages:
    - AUTHENTICATION REQUEST
    - AUTHENTICATION REJECT
    - IDENTITY REQUEST
    - LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
    - LOCATION UPDATING REJECT
    - CM SERVICE ACCEPT, if the following two conditions apply:
        - no other MM connection is established; and
        - the CM SERVICE ACCEPT is the response to a CM SERVICE REQUEST with CM SERVICE TYPE IE set to ‘emergency call establishment’
    - CM SERVICE REJECT
    - ABORT
- GMM messages:
    - AUTHENTICATION & CIPHERING REQUEST
    - AUTHENTICATION & CIPHERING REJECT
    - IDENTITY REQUEST
    - ATTACH REJECT

- ROUTING AREA UPDATE ACCEPT (at periodic rou~~o~~ting area update with no change of routing area or temporary identity)
- ROUTING AREA UPDATE REJECT
- SERVICE REJECT
- DETACH ACCEPT (for non power-off)

CC messages:

- all CC messages, if the following two conditions apply:
  - no other MM connection is established; and
  - the MM entity in the MS has received a CM SERVICE ACCEPT message with no ciphering or integrity protection applied as response to a CM SERVICE REQUEST message, with CM SERVICE TYPE set to 'Emergency call establishment' sent to the network.

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

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

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

4.1.1.1.1a Integrity protection for emergency call (UMTS only)

~~As a serving network option, t~~The network should~~shall~~ initiate the security mode procedure for an emergency call, in the same way as it would for any other call except in the cases defined in sub-clause "Security Procedures Not Applied" in TS 33.102.

For the establishment of a MM connection for an emergency call when no other MM connection is established (e.g. for an emergency call initiated without a SIM no other MM connections can exist) the decision on whether or not to apply the security procedures shall be made by the network as defined in the sub-clause "Emergency Call Handling" in TS 33.102.~~, the core network need not initiate a security mode control procedure for the CS domain in order to activate integrity protection.~~

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

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

*** Next Modified Sub-Clause ***

4.5.1 MM connection establishment

4.5.1.1 MM connection establishment initiated by the mobile station

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

- An MM connection establishment may only be initiated by the mobile station when the following conditions are fulfilled:

  - Its update status is UPDATED.

  - The MM sublayer is in one of the states MM IDLE or MM connection active but not in MM connection active (Group call).

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

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

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

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

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

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

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

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

c) Only applicable for mobile stations supporting VGCS talking:

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

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

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

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

The CM SERVICE REQUEST message contains the

- mobile identity according to section 10.5.1.4;
- mobile station classmark 2;
- ciphering key sequence number; and
- CM service type identifying the requested type of transaction (e.g. mobile originating call establishment, emergency call establishment, short message service, supplementary service activation, location services)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#4 : IMSI unknown in VLR

#6 : Illegal ME

#17 : Network failure

#22 : Congestion

#32 : Service option not supported

#33 : Requested service option not subscribed

#34 : Service option temporarily out of order

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

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

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

4.5.1.2 Abnormal cases

Mobile station side:

a) RR connection failure or IMSI deactivation

If an RR connection failure occurs or the IMSI is deactivated during the establishment of an MM connection, the MM connection establishment is aborted, timers T3230 is stopped, and an indication is given to the CM entity that requested the MM connection establishment. This shall be treated as a rejection for establishment of the new MM connection, and the MM sublayer shall release all active MM connections.

b) T3230 expiry

If T3230 expires (i.e. no response is given but a RR connection is available) the MM connection establishment is aborted and the requesting CM sublayer is informed. If no other MM connection exists then the mobile station shall proceed as described in section 4.5.3.1 for release of the RR connection. Otherwise the mobile station shall return to the MM sublayer state where the request of an MM connection was received, i.e. to MM sublayer state MM connection active. Other ongoing MM connections (if any) shall not be affected.

c) Reject cause values #95, #96, #97, #99, #100, #111 received

The same actions as on timer expiry shall be taken by the mobile station.

d) Random access failure or RR connection establishment failure

If the mobile station detects a random access failure or RR connection establishment failure during the establishment of an MM connection, it aborts the MM connection establishment and gives an indication to the CM entity that requested the MM connection establishment.

NOTE: Further actions of the mobile station depend on the RR procedures and MM specific procedures during which the abnormal situation has occurred and are described together with those procedures.

Network side:

a) RR connection failure

The actions to be taken upon RR connection failure within a MM common procedure are described together with that procedure. A RR connection failure occurring outside such MM common procedures, shall trigger the release of all active MM connections if any.

b) Invalid message or message content

Upon reception of an invalid initial message or a CM SERVICE REQUEST message with invalid content, a CM SERVICE REJECT message shall be returned with one of the following appropriate Reject cause indications:

# 95: Semantically incorrect message

# 96: Mandatory information element error

# 97: Message type non-existent or not implemented

# 99: Information element non-existent or not implemented

# 100: Conditional IE error

# 111: Protocol error, unspecified

When the CM SERVICE REJECT message has been sent, the network may start RR connection release if no other MM connections exist or if the abnormal condition also has influence on the other MM connections.

3GPP TSG-CN1 Meeting #14 ***Tdoc N1-001420***

revised N1-001336

Cardiff, Wales - 20 - 24 November, 2000

CR-Form-v3

CHANGE REQUEST

⌘	**24.008**	**CR**	**290**	⌘ rev	**r2**	⌘ Current version:	**4.0.0**	⌘

*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 ☒

Title: ⌘	Application of security procedures to emergency calls		
Source: ⌘	Vodafone, Siemens		
Work item code: ⌘	Security	***Date:*** ⌘	08-11-2000
Category: ⌘	A	***Release:*** ⌘	R4

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘ Following a CR against 33.102, sent for information by SA3 (in document N1-000991) it was noted that the stage two requirements for applying the security features to emergency calls have changed in such a way as to be mis-aligned with the stage three specifications in 24.008. The stage two requirements, in 33.102, now read:

6.4.9 Emergency call handling

PLMNs shall support an emergency call teleservice as defined in TS 22.003 which fulfils the additional service requirements defined in TS 22.101.

6.4.9.1 Security procedures applied

The security mode procedure shall be applied as part of emergency call establishment as defined in TS 24.008. Thus, integrity protection (and optionally ciphering) shall be applied as for a non-emergency call. If authentication of the (U)SIM fails for any reason, the emergency call shall proceed as in 6.4.9.2 d) below. Once the call is in progress with integrity protection (and optionally ciphering) applied, failure of integrity checking or ciphering is an unusual circumstance and must be treated in the same manner as other equipment failures, that is, the call will terminate.

6.4.9.2 Security procedures not applied

As a serving network option, emergency calls may be established without the network having to apply the security mode procedure as defined in TS 24.008.

The following are the only cases where the "security procedure not applied"

		option may be used : a) Authentication is impossible because the (U)SIM is absent b) Authentication is impossible because the serving network cannot obtain authentication vectors due to a network failure c) Authentication is impossible because the (U)SIM is not permitted to receive non-emergency services from the serving network (e.g. there is no roaming agreement or the IMSI is barred) d) Authentication is possible but the serving network cannot successfully authenticate the (U)SIM This CR aims to bring 24.008 into line with what is specified above.
Summary of change:	⌘	The Mobile Station must be ready to continue the signalling for an emergency call with or without the security procedures having been applied. The MSC will make the decision as to whether or not security is applied to the emergency call.
Consequences if not approved:	⌘	Mobiles will be manufactured in such a way that network operators and users may have to compromise their level of security.

Clauses affected:	⌘	4.1.1.1.1, 4.1.1.1.1a, 4.5.1			
Other specs affected:	⌘	□	Other core specifications	⌘	
		□	Test specifications		
		□	O&M Specifications		
Other comments:	⌘	An identical change to 24.008 v3.5.0 exists in N1-001335			

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. 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.

*** First Modified Sub-Clause ***

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

In UMTS only, integrity protected signalling is mandatory with one exception regarding emergency calls (see 4.1.1.1.1a). In UMTS only, all layer 3 protocols shall use integrity protected signalling once the security mode procedure has been successfully activated in the network and the MS. Integrity protection of all layer 3 signalling messages is the responsibility of lower layers. It is the network which activates integrity protection. This is done using the security mode control procedure (TS 25.331).

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

The CS and PS domains in the network and the MM and GMM layers in the MS, are not aware of whether integrity protection has been started in the lower layers by the other domain. It is mandatory for the network to initiate one security mode control procedure for the CS domain and one for the PS domain.

~~Not all MM/GMM messages are integrity protected. Therefore, the following MM/GMM messages shall be accepted by the MM and GMM entities of the MS if they are received, before the security mode control procedure for that domain is activated in the lower layers in the MS:~~

Except the messages listed below, no layer 3 signalling messages shall be processed by the receiving MM and GMM entities or forwarded to the CM entities, unless the security mode control procedure is activated for that domain.

- MM messages:
    - AUTHENTICATION REQUEST
    - AUTHENTICATION REJECT
    - IDENTITY REQUEST
    - LOCATION UPDATING ACCEPT (at periodic location update with no change of location area or temporary identity)
    - LOCATION UPDATING REJECT
    - CM SERVICE ACCEPT, if the following two conditions apply:
        - no other MM connection is established; and
        - the CM SERVICE ACCEPT is the response to a CM SERVICE REQUEST with CM SERVICE TYPE IE set to ‘emergency call establishment’
    - CM SERVICE REJECT
    - ABORT
- GMM messages:
    - AUTHENTICATION & CIPHERING REQUEST
    - AUTHENTICATION & CIPHERING REJECT
    - IDENTITY REQUEST
    - ATTACH REJECT

- ROUTING AREA UPDATE ACCEPT (at periodic rou~~o~~ting area update with no change of routing area or temporary identity)

- ROUTING AREA UPDATE REJECT

- —SERVICE REJECT

- DETACH ACCEPT (for non power-off)

CC messages:

- all CC messages, if the following two conditions apply:
    - no other MM connection is established; and
    - the MM entity in the MS has received a CM SERVICE ACCEPT message with no ciphering or integrity protection applied as response to a CM SERVICE REQUEST message, with CM SERVICE TYPE set to ‘Emergency call establishment’ sent to the network.

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

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

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

4.1.1.1.1a Integrity protection for emergency call (UMTS only)

The network should initiate the security mode procedure for an emergency call, in the same way as it would for any other call except in the cases defined in sub-clause “Security Procedures Not Applied” in TS 33.102.

For the establishment of a MM connection for an emergency call when no other MM connection is established (e.g. for an emergency call initiated without a SIM no other MM connections can exist) the decision on whether or not to apply the security procedures shall be made by the network as defined in the sub-clause “Emergency Call Handling” in TS 33.102.~~, the core network need not initiate a security mode control procedure for the CS domain in order to activate integrity protection.~~

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

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

*** Next Modified Sub-Clause ***

4.5.1 MM connection establishment

4.5.1.1 MM connection establishment initiated by the mobile station

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

- An MM connection establishment may only be initiated by the mobile station when the following conditions are fulfilled:

  - Its update status is UPDATED.

  - The MM sublayer is in one of the states MM IDLE or MM connection active but not in MM connection active (Group call).

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

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

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

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

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

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

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

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

c) Only applicable for mobile stations supporting VGCS talking:

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

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

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

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

The CM SERVICE REQUEST message contains the

- mobile identity according to section 10.5.1.4;
- mobile station classmark 2;
- ciphering key sequence number; and
- CM service type identifying the requested type of transaction (e.g. mobile originating call establishment, emergency call establishment, short message service, supplementary service activation, location services)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#4 : IMSI unknown in VLR

#6 : Illegal ME

#17 : Network failure

#22 : Congestion

#32 : Service option not supported

#33 : Requested service option not subscribed

#34 : Service option temporarily out of order

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

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

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

4.5.1.2 Abnormal cases

Mobile station side:

a) RR connection failure or IMSI deactivation

If an RR connection failure occurs or the IMSI is deactivated during the establishment of an MM connection, the MM connection establishment is aborted, timers T3230 is stopped, and an indication is given to the CM entity that requested the MM connection establishment. This shall be treated as a rejection for establishment of the new MM connection, and the MM sublayer shall release all active MM connections.

b) T3230 expiry

If T3230 expires (i.e. no response is given but a RR connection is available) the MM connection establishment is aborted and the requesting CM sublayer is informed. If no other MM connection exists then the mobile station shall proceed as described in section 4.5.3.1 for release of the RR connection. Otherwise the mobile station shall return to the MM sublayer state where the request of an MM connection was received, i.e. to MM sublayer state MM connection active. Other ongoing MM connections (if any) shall not be affected.

c) Reject cause values #95, #96, #97, #99, #100, #111 received

The same actions as on timer expiry shall be taken by the mobile station.

d) Random access failure or RR connection establishment failure

If the mobile station detects a random access failure or RR connection establishment failure during the establishment of an MM connection, it aborts the MM connection establishment and gives an indication to the CM entity that requested the MM connection establishment.

NOTE: Further actions of the mobile station depend on the RR procedures and MM specific procedures during which the abnormal situation has occurred and are described together with those procedures.

Network side:

a) RR connection failure

The actions to be taken upon RR connection failure within a MM common procedure are described together with that procedure. A RR connection failure occurring outside such MM common procedures, shall trigger the release of all active MM connections if any.

b) Invalid message or message content

Upon reception of an invalid initial message or a CM SERVICE REQUEST message with invalid content, a CM SERVICE REJECT message shall be returned with one of the following appropriate Reject cause indications:

# 95: Semantically incorrect message

# 96: Mandatory information element error

# 97: Message type non-existent or not implemented

# 99: Information element non-existent or not implemented

# 100: Conditional IE error

# 111: Protocol error, unspecified

When the CM SERVICE REJECT message has been sent, the network may start RR connection release if no other MM connections exist or if the abnormal condition also has influence on the other MM connections.