Document ***S3-000483***
S3-000465
S1-000504

3GPP TSG S1#9
Taastrup, 17-21 July 2000

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

CHANGE REQUEST

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

33.102	**CR**	**095R2**	Current Version:	3.5.0

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

For submission to:	TSG SA #9	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

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

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

Source: SA WG3 **Date:** 2000-08-01

Subject: Handling of emergency call

Work item: Security

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

Reason for change: The handling of emergency calls from a security point of view is not specified.

Clauses affected: 6.4.5, 6.4.9 (New clause)

Other specs affected:	Other 3G core specifications	☒	→ List of CRs:	24.008 CR207R1
	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:

Original CR submitted to SA#8 for approval by S3

Revision 1 produced during SA#8 by H Dettner, A Howell, M Walker, I Sharp

Draft Revision 2 produced by Vodafone

Revision 2 produced by G. Rose (Qualcomm) and P. Howard (Vodafone). Agreed ar S3#14

help.doc

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

6.4.5 Security mode set-up procedure

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

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

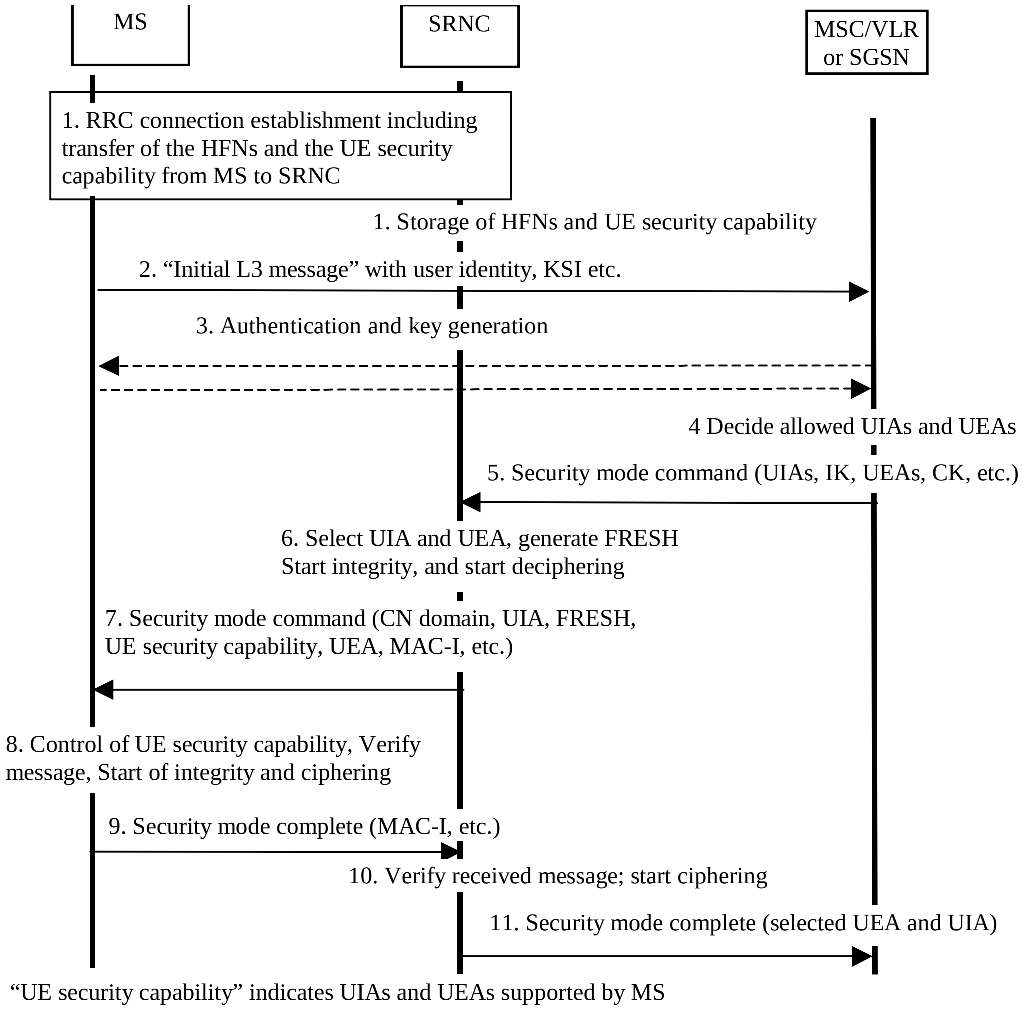
MS
SRNC
MSC/VLR or SGSN
1. RRC connection establishment including transfer of the HFNs and the UE security capability from MS to SRNC
1. Storage of HFNs and UE security capability
2. "Initial L3 message" with user identity, KSI etc.
3. Authentication and key generation
4 Decide allowed UIAs and UEAs
5. Security mode command (UIAs, IK, UEAs, CK, etc.)
6. Select UIA and UEA, generate FRESH Start integrity, and start deciphering
7. Security mode command (CN domain, UIA, FRESH, UE security capability, UEA, MAC-I, etc.)
8. Control of UE security capability, Verify message, Start of integrity and ciphering
9. Security mode complete (MAC-I, etc.)
10. Verify received message; start ciphering
11. Security mode complete (selected UEA and UIA)
"UE security capability" indicates UIAs and UEAs supported by MS

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "ME security capability" information before the integrity protection can start, i.e. the "ME security capability" must be sent to the network in an unprotected message. Returning the "ME security capability" later on to the ME in a protected message will give ME the possibility to verify that it was the correct "ME security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability and the initial hyperframe numbers (HFN) for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The initial HFN is used to initialise the HFN to be used as part of one of the input parameters COUNT-I for the integrity algorithm and COUNT-C, ,for the ciphering algorithm. The initial HFNs and the UE security capability information are stored in the SRNC.

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the MSC/VLR or SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The MSC/VLR or SGSN determines which UIAs and UEAs that are allowed to be used.

5. The MSC/VLR or SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. If ciphering shall be started, it contains the allowed UEAs and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of

new generated keys implies that the initial HFN to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the HFN already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, and the list of algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting MSC/VLR or SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the ME security capability received is equal to the ME security capability sent in the initial message. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the MSC/VLR or SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode complete from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the MS are integrity protected and possibly ciphered.

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the ME. The RNC is monitoring the COUNT-C and COUNT-I value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

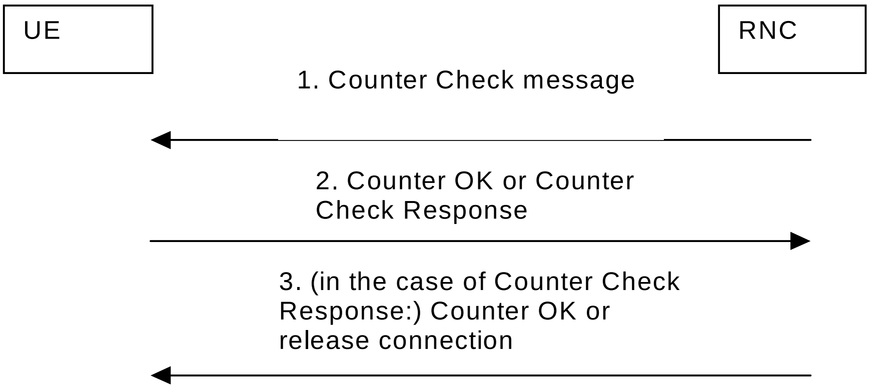
UE
RNC
1. Counter Check message
2. Counter OK or Counter Check Response
3. (in the case of Counter Check Response:) Counter OK or release connection

Figure 15a: RNC periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the RNC. The Counter Check message contains the most significant parts of the counter values (which reflect amount of data sent and received) from each active radio bearer.

2. The counter values in the Counter Check message are checked by ME and if they agree with the current status in the ME, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the ME and the values indicated in the Counter Check message, the ME sends a Counter Check response to the RNC. The form of this message is similar to the Counter Check message.

3. In case the RNC receives the 'Counter OK' message the procedure is completed. In case the RNC receives the Counter Check response it compares the counter values indicated in it to counter values in the RNC. If there is no difference or if the difference is acceptable then the RNC completes the procedure by sending the 'Counter OK' message. Otherwise, the connection is released.

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a START_{CS} value for the CS cipher/integrity keys and a START_{PS} value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the START_{CS} and the START_{PS} value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting START_{CS} and START_{PS} to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection), the RLC SN (for ciphering) and the MAC-d HFN (for ciphering) are initialised to 0.

During an ongoing radio connection, the START_{CS} value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling and CS user data logical channels protected using CK_{CS} and/or $\text{IK}_{\text{CS},}$ incremented by 1, i.e.:

$$\text{START}_{\text{CS}} = \text{MSB}_{20} \text{ (MAX \{COUNT-C, COUNT-I | all logical channels protected with } \text{CK}_{\text{CS}} \text{ and } \text{IK}_{\text{CS}}\text{\}) + 1.}$$

Likewise, during an ongoing radio connection, the START_{PS} value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling and PS user data logical channels protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$$\text{START}_{\text{PS}} = \text{MSB}_{20} \text{ (MAX \{COUNT-C, COUNT-I | all logical channels protected with } \text{CK}_{\text{PS}} \text{ and } \text{IK}_{\text{PS}}\text{\}) + 1.}$$

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates START$_{CS}$ and START$_{PS}$ in the USIM with the current values.

During authentication and key agreement the ME sets the START values of the corresponding service domain to 0 in the USIM and in the ME itself.

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