3GPP TSG-N meeting #7 **Tdoc 3GPP NP-000157**
Madrid, SPAIN
13 - 15 March 2000

Source: **Vodafone Airtouch**

Title: **CR 24.008-118r4 on Integrity checking of MM and GMM messages**

Agenda item: **5.1.3**

Document for: Approval

This contribution contains CR 24.008-118r4 on Integrity checking of MM and GMM messages. Revision 3 of this CR was agreed by N1 at their last meeting, but after the meeting it was noted that the CR had inserted some redundant text. This text has been struck out in the attached version of the CR. CN plenary are asked to approve the attached CR in place of revision 3, which is in document NP-000100 as N1-000534.

3GPP TSG CN Meeting #7
Madrid, Spain, 13 – 15 March.2000

Document NP-000
(previously N1-000534)

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**	**118r4**	Current Version:	3.2.1

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

For submission to: CN #7 *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 [ ]

Source: Vodafone Airtouch **Date:** 15/02/2000

Subject: Integrity checking of MM and GMM messages

Work item: Security

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

F	Correction	[ ]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change:

It is a requirement of UMTS that signalling messages be integrity protected. This protection allows the receiving entity to be sure that the messages are from a genuine source, and thus guards against 'replay attacks.'
All protocols shall use integrity protection, and integrity protection is mandatory even in networks where encryption is not turned on.

The receiving entity (MS or RNC) uses a secret key, obtained from and known only by the SIM and the HLR/Auc, to check the integrity 'signature' of a message. Lower layers are responsible for carrying out such checks and, in general, every signalling message received will be discarded by the lower layers if it does not pass the check. However, there are certain messages in MM/GMM that should be allowed up to the layer 3 entity, without having been successfully checked. (This may be because no keys have been agreed yet, or because ciphering and integrity has not been activated yet). On the other hand, there is also a case where, in a network which does not use encryption, certain messages must never be processed at layer 3 unless they have been successfully integrity checked.

Therefore, it is necessary in MM/GMM to run integrity checking almost on a per-message basis.

Clauses affected: 4.1.1.1

Other specs affected:

Other 3G core specifications	[X]	→ List of CRs:	24.007 – CR010
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.

Elementary procedures for Mobility Management

4.1 General

This section describes the procedures used for mobility management for non-GPRS services and for GPRS-services at the radio interface (Reference Point Um and Uu).

The main function of the Mobility Management sublayer is to support the mobility of user terminals, such as informing the network of its present location and providing user identity confidentiality.

A further function of the MM sublayer is to provide connection management services to the different entities of the upper Connection Management (CM) sublayer (see TS 24.007).

There are two sets of procedures defined in this chapter:

- MM procedures for non-GPRS services (performed by the MM entity of the MM sublayer); and
- GMM procedures for GPRS services (performed by the GMM entity and GMM-AA entity of the MM sublayer), see TS 24.007 [20].

All the MM procedures described in this section can only be performed if a RR connection has been established between the MS and the network. Else, the MM sublayer has to initiate the establishment of a RR connection (see GSM 04.18 section 3.3 and TS 25.331 section 8.2.3). The GMM procedures described in this section, use services provided by the RR sublayer without prior RR connection establishment.

GMM procedures are mandatory and applicable only for GPRS MSs and networks supporting those MSs. For GPRS MSs which are IMSI attached for both GPRS and non-GPRS services, some MM procedures are replaced by GMM combined procedures provided that the network operates in network operation mode I, i.e. is supporting combined GMM procedures. GMM combined procedures are not applicable for the GPRS MS operation mode C but are mandatory for the GPRS MS operation modes A and B and networks supporting network operation mode I, see TS 23.060.

4.1.1 MM and GMM procedures

4.1.1.1 Types of MM and GMM procedures

Depending on how they can be initiated, three types of MM procedures can be distinguished:

1) MM common procedures:
   A MM common procedure can always be initiated whilst a RR connection exists. The procedures belonging to this type are:
   Initiated by the network:
   - TMSI reallocation procedure;
   - authentication procedure;
   - identification procedure;
   - MM information procedure;
   - abort procedure.
     However, abort procedure is used only if an MM connection is being established or has already been established i.e. not during MM specific procedures or during IMSI detach procedure, see section 4.3.5.

   Initiated by the mobile station:
   - IMSI detach procedure (with the exceptions specified in section 4.3.4).

ii) MM specific procedures:
   A MM specific procedure can only be initiated if no other MM specific procedure is running or no MM connection exists. The procedures belonging to this type are:
   - normal location updating procedure;
   - periodic updating procedure;
   - IMSI attach procedure.

iii) MM connection management procedures:

These procedures are used to establish, maintain and release a MM connection between the mobile station and the network, over which an entity of the upper CM layer can exchange information with its peer. A MM

connection establishment can only be performed if no MM specific procedure is running. More than one MM connection may be active at the same time. Depending on how they can be initiated, two types of GMM procedures can be distinguished:

i) GMM common procedures:

Initiated by the network when a GMM context has been established:

- P-TMSI (re-) allocation;
- GPRS authentication and ciphering;
- GPRS identification;
- GPRS information.

ii) GMM specific procedures:

Initiated by the network and used to detach the IMSI in the network for GPRS services and/or non-GPRS services and to release a GMM context:

- GPRS detach.

Initiated by the MS and used to attach or detach the IMSI in the network for GPRS services and/or non-GPRS services and to establish or release a GMM context:

- GPRS attach and combined GPRS attach;
- GPRS detach and combined GPRS detach.

Initiated by the MS when a GMM context has been established:

- normal routing area updating and combined routing area updating;
- periodic routing area updating.

4.1.1.1.1 Integrity Checking of Signalling Messages in the Mobile Station

In UMTS only, integrity protected signalling is mandatory. In UMTS only, all protocols shall use integrity protected signalling. 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).

MM and GMM signalling messages have to be checked for integrity by the MS on a per-message basis. Some MM/GMM messages shall be processed regardless of whether or not integrity protection was activated. Lower layers in the MS provide MM/GMM with an indication for every MM/GMM message as to the result of the integrity checking process:

No integrity check performed;
Integrity check performed and was successful; or
Integrity check performed and was unsuccessful.

Integrity checking on the network side is performed by the RNC and is described in TS 25.413

Not all MM/GMM messages are integrity protected. Therefore, the following MM/GMM messages shall not be discarded by the MM/GMM entity of the MS, regardless of whether they pass or fail the integrity check:

MM messages:

- AUTHENTICATION REQUEST
- ~~AUTHENTICATION FAILURE~~
- AUTHENTICATION REJECT
- IDENTITY REQUEST
- LOCATION UPDATING REJECT
- CM SERVICE REJECT

GMM messages:

- AUTHENTICATION & CIPHERING REQUEST
- ~~AUTHENTICATION & CIPHERING FAILURE~~
- AUTHENTICATION & CIPHERING REJECT
- IDENTITY REQUEST
- ATTACH REJECT
- ROUTING AREA UPDATE REJECT
- SERVICE REJECT (UMTS only)

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. If any signalling messages, having not successfully passed the integrity check, are received by layer 3, the MS shall discard that message.