CHANGE REQUEST No :	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM / UMTS: 03.20   Version: 7.1.0

Submitted to SMG #32   for approval **X**   without presentation ("non-strategic") **X**
list SMG plenary meeting no. here ↑   for information   with presentation ("strategic")

PT SMG CR cover form. Filename: crf26_3.doc

Proposed change affects: SIM ☐ ME **X** Network **X**
(at least one should be marked with an X)

Work item: GPRS

Source: SMG10   **Date:** 2000-01-22

Subject: GPRS encryption

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

Reason for change: It is required to clarify that A5 ciphering of the data stream at layer 1 is not supported on GPRS channels.

Clauses affected: 2.3.9

Other specs Affected:
Other releases of same spec	☐	→ List of CRs:
Other core specifications	☐	→ List of CRs:
MS test specifications / TBRs	☐	→ 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.

2.3.9   Combined location area updating with the routing area updating

This subclause is only applicable if GPRS is supported.

This procedure is part of the location updating of a General Packet Radio Service (GPRS) class A or B mobile when the Gs-interface (SGSN MSC/VLR signalling interface) is implemented. This procedure is not relevant if the Gs-interface is not implemented.

The location area updating procedure and the routing area updating procedure are combined to one MS Serving GPRS Support Node (SGSN) procedure. The MS includes a Location Area Update (LAU) indication in the Routing Area Update Request message. The SGSN performs the location updating towards the VLR on behalf of the MS.

The procedure described in figure 2.8 shows only the interaction between the SGSN and the VLR. The full procedure including the update to other network element (e.g. HLR, old MSC/VLR) is described in GSM 03.60 .

```
 ........  ...............  ..............        ...........
 • MS  • •     BSS     • •    SGSN     •        •   VLR   •
 ........  ...............  ..............        ...........á
    •                           ••                   •      á
    • RAI, TLLI, LAU indication ••                   •
    •••••••••••••••••••••••••••••>••                  •
    •   (note 1)                 ••                   •
    •                        ..............           •
    •                        •  Security  •á          •
    •                        •  functions •           •
    •                        ..............           •      á
    •                           ••                    •
    •                           •• IMSI,LAI (note 2)  •
    •                           ••••••••••••••••••••••>•
    •                           ••               ..............
    •                           ••               •  Allocation •
    •                           ••               •   of TMSIn  •
    •                           ••               ..............
    •                           ••                   •
    •                           ••    TMSIn (note 3) •
    •                           ••<•••••••••••••••••••
    •                           ••                   •      á
    •                           ••                   •
    •    Cipher(TMSIn)(note 4)  ••                   •
    •<•••••••••••••••••••••••••••••                  •á
    •                           ••                   • á
    •                           ••                   • á
    •   Acknowledge (note 5)    ••Acknowledge(note 6)• á
    •••••••••••••••••••••••••••••>••••••••••••••••••••>•• á
    •                               ..............
    •                               •Deallocation•á
    •                               •of TMSIo     •
    •                               ..............
```

NOTE 1: The Routeing Area Update Request message including the old Routing Area Identifier (RAI), the Temporary Logical Link Identifier (TLLI), and an indication that a combined Location Area Update (LAU) is performed.

NOTE 2: Location Updating message.

NOTE 3: Location Updating Accept message including the new TMSI.

NOTE 4: Routing Area Update Accept message including the new TMSI and the new TLLI (if any).

NOTE 5: Routing Area Update Complete message including the TLLI and TMSI.

NOTE 6: TMSI Reallocation Complete message including the TMSI.

Figure 2.8: Combined routing area and location updating in the same VLR

When the VLR does not change the TMSI, the old TMSI will stay in use and there is no need to send any TMSI to the MS.

In case of combined routing area update and inter-VLR location area updating procedure, the old TMSI will be cancelled and the HLR is updated as described in GSM 03.60.

If the Location Updating message indicates a reject (if for example the MS try to enter a forbidden location area), then this should be indicated to the MS and the MS shall not access non-GPRS service until a successful Location Update is performed.

For the combined location and routing area update and the combined GPRS Attach and IMSI Attach for GPRS class A and B mobiles, the authentication is performed by the SGSN. The authentication procedure for GPRS is described in annex D. The MSC/VLR relies on the SGSN authentication. This authentication procedure generates no ciphering key for circuit switched ciphering.

The ciphering key for circuit switched operation is allocated through an authentication by MSC/VLR when the circuit switched service is requested. Also, the MSC/VLR may use the old ciphering key if existing.

For clarification, A5 ciphering of the data stream at layer 1 is not supported on GPRS channels.