**3GPP TSG-SA WG3 Meeting #16** **S3-000739**
**Sophia Antipolis, France, 28-30 November 2000**

*CR-Form-v3*

# CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **3.6.0** ⌘

*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 **X** Radio Access Network ☐ Core Network ☐

| | | |
|---|---|---|
| ***Title:*** | ⌘ | START value handling for MS with a GSM SIM inserted |
| ***Source:*** | ⌘ | Vodafone |
| ***Work item code:*** | ⌘ | Security ***Date:*** ⌘ 30-Nov-00 |
| ***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:*** | ⌘ | It needs to be specified what START value is used to initialise the hyperframe number which is input to the confidentiality and integrity algorithms when a GSM SIM is inserted into a UMTS terminal (when a USIM is inserted the START value is read from the USIM). |
| ***Summary of change:*** | ⌘ | Section 6.8.2.4 is modified to specify that START values are stored in the ME when a GSM SIM is inserted. |
| ***Consequences if not approved:*** | ⌘ | It would not be possible to use a 3G ME with a GSM SIM card inserted on UTRAN. |

| | | | | |
|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.8.2.4 | | |
| ***Other specs affected:*** | ⌘ | **X** Other core specifications | ⌘ | TS 25.331 |
| | | **X** Test specifications | | TS 34.123, TS 34.108 |
| | | ☐ 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.

### 6.8.2.3 VLR/SGSN

The R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited VLR/SGSN.

NOTE: All triplets are originally provided by the HLR/AuC.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

When the user is attached to a UTRAN, the R99+ VLR/SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) c4: $CK_{[UMTS]}$ = Kc || Kc;

b) c5: $IK_{[UMTS]}$ = $Kc_1$ xor $Kc_2$ || Kc || $Kc_1$ xor $Kc_2$;

whereby in c5, $Kc_i$ are both 32 bits long and Kc = $Kc_1$ || $Kc_2$.

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the cipher key Kc is applied in the SGSN itself.

### 6.8.2.4 R99+ ME

R99+ ME with a SIM inserted, shall participate only in GSM AKA.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ME.

When the user is attached to a UTRAN, R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc using the conversion functions c4 and c5. The ME shall handle the $START_{CS}$ and $START_{PS}$ as described in section 6.4.8 with the exception that the START values are stored on the ME rather than on the GSM SIM. If the ME looses the current START value for a particular domain (e.g. due to power off) it shall delete the corresponding GSM cipher key (Kc), the derived UMTS cipher/integrity keys (CK and IK), and reset the START value to zero. The ME shall then trigger a new authentication and key agreement at the next connection establishment by indicating to the network that no valid keys are available for use using the procedure described in section 6.4.4.