3GPP TSG SA WG 3 (Security) meeting #15
Washington (USA), 12—14 September, 2000

Document **S3-000544**
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**	**xxx**	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:	SA #9	for approval	X	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: *(at least one should be marked with an X)* (U)SIM [ ] ME [X] UTRAN / Radio [ ] Core Network [ ]

Source: QUALCOMM Incorporated **Date:** 2000-09-06

Subject: START value handling for ME

Work item: Security

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

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

Release:

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

Reason for change: Clarification needed on the handling of $START_{CS}$ and $START_{PS}$ so that only appropriate one is reset.

Clauses affected: 6.8.2.4

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
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

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~~ or the $START_{PS}$ value as appropriate to the RNC in the *RRC connection setup complete* message. The ME marks the corresponding START value~~s~~ in the USIM as invalid by setting $START_{CS}$ ~~and~~ or $START_{PS}$ 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) and~~,~~ 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 $IK_{CS,}$ incremented by 1, i.e.:

$START_{CS} = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all logical channels protected with CK_{CS} and IK_{CS}}) + 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.:

$START_{PS} = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all logical channels protected with CK_{PS} and IK_{PS}}) + 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.

6.8.2.4 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.