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

S3-000664

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 ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Correction for integrity protection when using GSM SIM cards in UMTS ME.			
Source:	⌘	Nokia			
Work item code:	⌘	Security	***Date:***	⌘	20-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 has been idea since the beginning of the UMTS, that it's possible to use GSM SIM cards on UMTS MEs. However, GSM SIM card is missing essential file $EF_{THRESHOLD}$ (Maximum value of START) which is required in integrity protection. All the other keys in integrity protection may be computed by ME.
Summary of change:	⌘	Chapter 6.4.3 modified to support also GSM SIM cards. Chapter 6.8.2.4 modified to support receiving of maximum value of START. Annex F.3 modified according to changes in ch. 6.4.3.
Consequences if not approved:	⌘	It's not possible to use UMTS MEs with GSM SIM cards on UTRAN.

Clauses affected:	⌘	6.4.3, 6.8.2.4 and annex F.3	
Other specs affected:	⌘	☒ Other core specifications ☒ Test specifications □ O&M Specifications	⌘ TS 24.008 TS 34.123
Other comments:	⌘		

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set. In case that the maximum value of of START$_{CS}$ and/or START$_{PS}$ is not available from the SIM/USIM, network may send information for the ME to limit the amount of data that is protected by an access link key set. The ME shall use this received information only in the case that the limiter value is not available from the SIM/USIM.

Each time an RRC connection is released the values START$_{CS}$ and START$_{PS}$ of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM.

The ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) at the next RRC connection request message sent out if START$_{CS}$ or START$_{PS}$ has reached a maximum value set by the operator and stored in the USIM, or set by the operator, sent from the network to the ME and stored in the ME~~ at the next RRC connection request message sent out~~. The ME shall use this received information only in the case that the limiter value is not available from the SIM/USIM. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

************ Next modification ************

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. R99+ ME shall store the maximum value of START$_{CS}$ and/or START$_{PS}$ if they are received from network e.g. in AUTHENTICATION REQUEST message as optional information element.

************ Next modification ************

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM, or ME assisted by network in case that SIM/USIM does not support this mechanism, contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.