3GPP TSG-SA WG 3 Security - S3#18
Phoenix, USA, 21-24. May 2001

S3-010184

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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 to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted		
Source:	⌘	Nokia		
Work item code:	⌘	Security	***Date:*** ⌘	17-05-01
Category:	⌘	**A**	***Release:*** ⌘	REL-4

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 is possible to use SIM cards on UMTS MEs. However, even release 99 SIM card is missing essential file $EF_{THRESHOLD}$ (Maximum value of START) which is required in integrity protection. As a consequence, a default value should be used on ME when the user is attached to a UTRAN with R99+ ME with a SIM inserted.
Summary of change:	⌘	Chapter 6.4.3 modified to support also SIM cards. Chapter 6.8.2.4 modified to use a default value for the maximum value of $START_{CS}$ or $START_{PS}$. Annex F.3 modified according to changes in ch. 6.4.3.
Consequences if not approved:	⌘	It is not possible to use SIM cards on UMTS MEs.

Clauses affected:	⌘	6.4.3, 6.8.2.4 and annex F.3	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ 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.

6.4.3 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.

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) if START$_{CS}$ or START$_{PS}$ has reached a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out. 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.

When the user is attached to a UTRAN, R99+ ME with a SIM inserted shall use a default value for maximum value of START$_{CS}$ or START$_{PS}$ as described in chapter 6.8.2.4.

********** **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. 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.

When the user is attached to a UTRAN, R99+ ME with a SIM inserted shall use a default value of all ones for maximum value of START$_{CS}$ or START$_{PS}$. The ME shall handle the maximum value of START$_{CS}$ or START$_{PS}$ as described in section 6.4.3 with the exception that the maximum value of START$_{CS}$ or START$_{PS}$ is stored on the ME rather than on the GSM SIM.

********** **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 a R99+ ME with a SIM card inserted 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.