3GPP TSG-SA WG3 Meeting #18
Phoenix, USA, 21st – 24th May 2001

S3-010238
(Part 2: Rel-4 CR)

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 [X] ME/UE [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	THRESHOLD Check at RRC connection establishment.
Source:	⌘	SA WG3
Work item code:	⌘	Security Architecture
Date:	⌘	21-May-01
Category:	⌘	**A**
Release:	⌘	R4

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:	⌘	Initial “L3 message” might be prepared before request of RRC connection establishment so it might contain a valid KSI even when the START values have reached THRESHOLD (R2-010981).
Summary of change:	⌘	Main changes includes: - Edictorial changes, - THRESHOLD value is checked at RRC connection release (START values are set to invalid and Keys are deleted if THRESHOLD is reached).
Consequences if not approved:	⌘	Use of THRESHOLD is not serving its purpose and old keys are used in an additional RRC connection.

Clauses affected:	⌘	6.4.3		
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	
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.

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. If $START_{CS}$ or $START_{PS}$ have reached a maximum value (THRESHOLD), the ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD. When this maximum value is reached the cipher key and integrity key stored on the USIM shall be deleted. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established, ~~that~~ START values are read from the USIM. Then, 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~~ the maximum value THRESHOLD, ~~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.