

## 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

<b>Title:</b>	⌘ Calculation and Wrap-around of START value		
<b>Source:</b>	⌘ SA WG3		
<b>Work item code:</b>	⌘ Security Architecture	<b>Date:</b>	⌘ 23-May-01
<b>Category:</b>	⌘ <b>A</b>	<b>Release:</b>	⌘ R4
	<i>Use <u>one</u> of the following categories:</i> <b>F</b> (essential correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (Addition of feature), <b>C</b> (Functional modification of feature) <b>D</b> (Editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900.		<i>Use <u>one</u> of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ Clarifications on the handling of wrap-around of START values and in its calculation.		
<b>Summary of change:</b>	⌘ According to 25.331 (chapter 8.5.9), during the calculation of the START value for a CN domain 'x' (being START <sub>x</sub> the new calculated value of START) ... "if the current START <sub>x</sub> < START <sub>x</sub> ', then START <sub>x</sub> = START <sub>x</sub> ', otherwise START <sub>x</sub> is unchanged". This is done in order to avoid that START values decrease between two calculations. This note is now added in 33.102.  If any of the COUNT values assigned to the radio bearers of the same CN domain wraps around, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.		
<b>Consequences if not approved:</b>	⌘ R2 and S3 specs will not be aligned. Additionally wrap-around conditions in START values will not be considered.		

<b>Clauses affected:</b>	⌘ 6.4.8		
<b>Other specs affected:</b>	⌘ <input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘ 25.331	
<b>Other comments:</b>	⌘		

## 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 the  $START_{PS}$  value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting  $START_{CS}$  and  $START_{PS}$  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) are initialised to 0.

During an ongoing radio connection, the  $START_{CS}$  value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using  $CK_{CS}$  and/or  $IK_{CS}$ , incremented by 1, i.e.:

$$START_{CS}' = MSB_{20} ( \text{MAX} \{ \text{COUNT-C, COUNT-I} \mid \text{all radio bearers (including signalling) protected with } CK_{CS} \text{ and } IK_{CS} \} ) + 1.$$

- If current  $START_{CS} < START_{CS}'$  then  $START_{CS} = START_{CS}'$ , otherwise  $START_{CS}$  is unchanged.

Likewise, during an ongoing radio connection, the  $START_{PS}$  value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using  $CK_{PS}$  and/or  $IK_{PS}$ , incremented by 1, i.e.:

$$START_{PS}' = MSB_{20} ( \text{MAX} \{ \text{COUNT-C, COUNT-I} \mid \text{all radio bearers (including signalling) protected with } CK_{PS} \text{ and } IK_{PS} \} ) + 1.$$

- If current  $START_{PS} < START_{PS}'$  then  $START_{PS} = START_{PS}'$ , otherwise  $START_{PS}$  is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

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 START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.