3GPP TSG-SA WG3 Meeting #20
Sydney, Australia, 16-19 October 2001

Tdoc S3-010474

CR-Form-v4

CHANGE REQUEST

⌘ **33.102 CR zzz** ⌘ ev **-** ⌘ Current version: **3.9.0** ⌘

*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: ⌘	Alignments with 25.331		
Source: ⌘	Nokia		
Work item code: ⌘		***Date:*** ⌘	9 Oct 01
Category: ⌘	**F**	***Release:*** ⌘	R99
	Use one of the following categories: ***F*** *(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: ⌘ Inconsistency between 33.102 and 25.331 regarding the lifetime of ciphering and integrity keys. In 33.102 it is specified that when START **reaches** THRESHOLD, ciphering and integrity keys are deleted.
However in 25.331 chapter 8.5.2 it is specified that:

When entering idle mode, the UE shall:

- if the USIM is present:
  - store the current START value for every CN domain in the USIM [50];
  - if the "START" stored in the USIM [50] for a CN domain **is greater than** the value "THRESHOLD" of the variable START_THRESHOLD:
    - delete the ciphering and integrity keys that are stored in the USIM for that CN domain;
    - inform the deletion of these keys to upper layers.

Summary of change: ⌘ 33.102 has been aligned with 25.331:

- "reached" changed to "greater than"
- clarification in START value calculation

Consequences if not approved: ⌘ Inconsistency between specifications.

Clauses affected: ⌘	6.4.3, 6.4.8, 6.5.4.2, 6.6.4.2		
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://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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 compared with the maximum value, THRESHOLD. If START_{CS} ~~and/~~or START_{PS} ~~have reached~~is greater than the maximum value (THRESHOLD), the ME ~~marks the START value in the USIM for the corresponding core network domain(s) as invalid by setting the START_{CS} and/or START_{PS} to THRESHOLD, ~~deletes the cipher key and the integrity key for the corresponding core network domain stored on the USIM and sets the KSI to invalid (refer to section 6.4.4). Otherwise, the START_{CS} and START_{PS} are stored in the USIM. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established, 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 for the corresponding core network domain) if the access link key set has been deleted~~START_{CS} and/or START_{PS} has reached the maximum value, THRESHOLD, for the corresponding core network domain(s)~~.

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, a R99+ ME with a SIM inserted shall use a default value for maximum value of START_{CS} or START_{PS} as described in section 6.8.2.4.

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$_{\text{CS}}$ value for the CS cipher/integrity keys and a START$_{\text{PS}}$ 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$_{\text{CS}}$ and the START$_{\text{PS}}$ 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$_{\text{CS}}$ and START$_{\text{PS}}$ 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$_{\text{CS}}$ 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 the most recently configured CK$_{\text{CS}}$ and/or IK$_{\text{CS,}}$ incremented by 1, i.e.:

START$_{\text{CS}}$' = MSB$_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with the most recently configured CK$_{\text{CS}}$ and IK$_{\text{CS}}$}) + 1.

- If current START$_{\text{CS}}$ < START$_{\text{CS}}$' then START$_{\text{CS}}$ = START$_{\text{CS}}$', otherwise START$_{\text{CS}}$ is unchanged.

Likewise, during an ongoing radio connection, the START$_{\text{PS}}$ 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 the most recently configured CK$_{\text{PS}}$ and/or IK$_{\text{PS}}$, incremented by 1, i.e.:

START$_{\text{PS}}$' = MSB$_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with the most recently configured CK$_{\text{PS}}$ and IK$_{\text{PS}}$}) + 1.

- If current START$_{\text{PS}}$ < START$_{\text{PS}}$' then START$_{\text{PS}}$ = START$_{\text{PS}}$', otherwise START$_{\text{PS}}$ 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$_{\text{CS}}$ and START$_{\text{PS}}$ 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.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

For signalling radio bearers (RB 0-4) there is one COUNT-I value per up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. The "short" sequence number is the 4-bit RRC sequence number (RRC SN) that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.

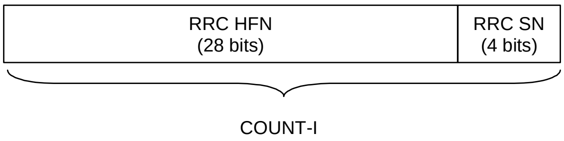

Figure 16a: The structure of COUNT-I

The RRC HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.5.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that a valid IK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM are not up-to-date or $START_{CS}$ or $START_{PS}$ ~~have reached~~is greater than THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSNas part of a quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) *security mode command*.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation (see TS 25.331 [17]).

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. For all transparent mode RLC radio bearers of the same CN domain COUNT-C is the same, and COUNT-C is also the same for uplink and downlink.

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

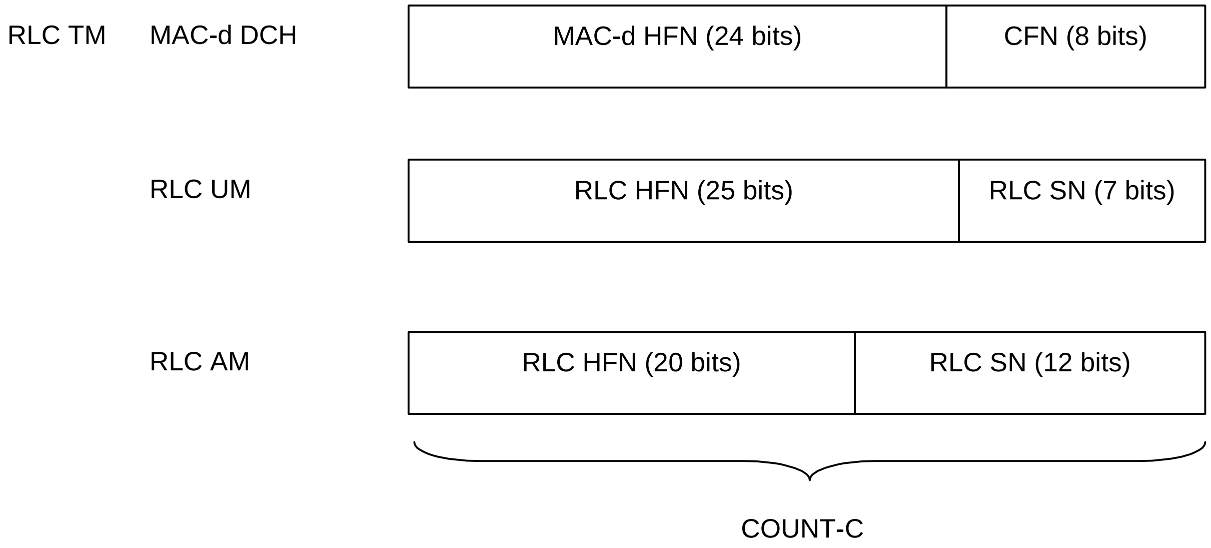

Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.
- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. The "long" sequence number is the 25-bit RLC UM HFN which is incremented at each RLC SN cycle.
- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number (RLC SN) and this is part of the RLC AM PDU header. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START. The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

When a new radio bearer is created during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see section 6.4.8).

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. The CK to use for a particular radio bearer is described in 6.6.5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that a valid CK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM ~~have reached~~is greater than THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSN as part of the quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.