**3GPP TSG-RAN2 Meeting #110-e draftR2-200xx**

**Online, 1-12 June, 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.331** | **CR** | **1555** | **rev** | **2** | **Current version:** | **15.9.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on avoiding keystream repeat due to COUNT reuse | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, Ericsson, Vodafone, NTT DOCOMO | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NR\_newRAT-Core | | | | |  | ***Date:*** | | | 2020-05-21 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-15 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change 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](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | TS 33.501 mandates the avoidance of keystream repeat (see below text with added highlighting)  “Key refresh shall be possible for KgNB, KRRC-enc, KRRC-int, KUP-enc, and KUP-int (if available ) and shall be initiated by the gNB/ng-eNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same KgNB.”  In TS 38.331, while it is stated that “It is not allowed to use the same COUNT value more than once for a given security key.” and “The network is responsible for avoiding reuse of the COUNT with the same RB identity and with the same KeNB”, the reference to TS 33.501 is missing and there is possibility of misunderstanding that the requirement s are described within this specification (TS 38.331). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Add reference to TS 33.501 regarding avoidance of keystream repeat. 2. Move text about HFN to next pragraph in order to keep the related texts about COUNT together for clarity.   **Impact Analysis:**  **Impacted Functionality:**  AS Security  **Interoperability:**   1. As the changes align RRC specs with existing SA3 requirements, no interoperability issue is foreseen. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | RAN2 specification remains misaligned with SA3 specifications. As the reference to TS 33.501 is missing, there is possibility of misunderstanding that the requirements are described in TS 38.331 instead of TS 33.501. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

First change

#### 5.3.1.2 AS Security

AS security comprises of the integrity protection and ciphering of RRC signalling (SRBs) and user data (DRBs).

RRC handles the configuration of the AS security parameters which are part of the AS configuration: the integrity protection algorithm, the ciphering algorithm, if integrity protection and/or ciphering is enabled for a DRB and two parameters, namely the *keySetChangeIndicator* and the *nextHopChainingCount*, which are used by the UE to determine the AS security keys upon reconfiguration with sync (with key change), connection re-establishment and/or connection resume.

The integrity protection algorithm is common for SRB1, SRB2, SRB3 (if configured) and DRBs configured with integrity protection, with the same *keyToUse* value. The ciphering algorithm is common for SRB1, SRB2, SRB3 (if configured) and DRBs configured with the same *keyToUse* value. For MR-DC, integrity protection is not enabled for DRBs terminated in eNB. Neither integrity protection nor ciphering applies for SRB0.

NOTE 0: All DRBs related to the same PDU session have the same enable/disable setting for ciphering and the same enable/disable setting for integrity protection, as specified in TS 33.501 [11].

RRC integrity protection and ciphering are always activated together, i.e. in one message/procedure. RRC integrity protection and ciphering for SRBs are never de-activated. However, it is possible to switch to a '*NULL*' ciphering algorithm (*nea0*).

The '*NULL*' integrity protection algorithm (*nia0*) is used only for SRBs and for the UE in limited service mode, see TS 33.501 [11] and when used for SRBs, integrity protection is disabled for DRBs. In case the ′*NULL*' integrity protection algorithm is used, '*NULL*' ciphering algorithm is also used.

NOTE 1: Lower layers discard RRC messages for which the integrity protection check has failed and indicate the integrity protection verification check failure to RRC.

The AS applies four different security keys: one for the integrity protection of RRC signalling (KRRCint), one for the ciphering of RRC signalling (KRRCenc), one for integrity protection of user data (KUPint) and one for the ciphering of user data (KUPenc). All four AS keys are derived from the KgNB key. The KgNB key is based on the KAMF key (as specified in TS 33.501 [11]), which is handled by upper layers.

The integrity protection and ciphering algorithms can only be changed with reconfiguration with sync. The AS keys (KgNB, KRRCint, KRRCenc, KUPint and KUPenc) change upon reconfiguration with sync (if *masterKeyUpdate* is included), and upon connection re-establishment and connection resume.

For each radio bearer an independent counter (*COUNT*, as specified in TS 38.323 [5]) is maintained for each direction. For each radio bearer, the *COUNT* is used as input for ciphering and integrity protection.

It is not allowed to use the same *COUNT* value more than once for a given security key. As specified in TS 33.501 subclause 6.9.4.1 [11], the network is responsible for avoiding reuse of the *COUNT* with the same RB identity and with the same key, e.g. due to the transfer of large volumes of data, release and establishment of new RBs, and multiple termination point changes for RLC-UM bearers. In order to avoid such re-use, the network may e.g. use different RB identities for RB establishments, change the AS security key, or an RRC\_CONNECTED to RRC\_IDLE/RRC\_INACTIVE and then to RRC\_CONNECTED transition.

For each SRB, the value provided by RRC to lower layers to derive the 5-bit BEARER parameter used as input for ciphering and for integrity protection is the value of the corresponding *srb-Identity* with the MSBs padded with zeroes.

For a UE provided with an *sk-counter*, *keyToUse* indicates whether the UE uses the master key (KgNB) or the secondary key (S-KeNB or S-KgNB) for a particular DRB. The secondary key is derived from the master key and *sk-Counter*, as defined in 33.501[86]. Whenever there is a need to refresh the secondary key, e.g. upon change of MN with KgNB change or to avoid COUNT wrap around, the security key update is used (see 5.3.5.7). When the UE is in NR-DC, the network may provide a UE configured with an SCG with an *sk-Counter* even when no DRB is setup using the secondary key (S-KgNB) in order to allow the configuration of SRB3. The network can also provide the UE with an *sk-Counter*, even if no SCG is configured, when using SN terminated MCG bearers.

End of Changes