**3GPP TSG-RAN WG2 Meeting #109bis-e *R2-200xxxx***

**Elbonia, 20 – 30 April 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **36.331** | **CR** | **4241** | **rev** | **1** | **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:*** | Avoiding security risk for RLC AM and RLC UM bearers during termination point change | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Deutsche Telekom | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NR\_newRAT-Core | | | | |  | ***Date:*** | | | 2020-02-27 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | 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:*** | | During the discussion on R2-1816725, it was decided that the network must ensure that the COUNT is not reused to avoid security risk for RLC UM. In this discussion the RLC AM was excluded as it was understood that the COUNT reuse will not happen even in the case of multiple termination point changes as the PDCN SN is continued. However, in our understanding, for the following example scenario, this is no longer true in the following scenario where the For RLC-AM bearers, multiple termination point consecutive changes can result in PDCP COUNT cannot be maintained for the same DRBid in the case SN terminated PDCP reset due to SN only full configuration:   |  | | --- | | 1. Bearer starts in eNB as MCG bearer with RLC AM (e.g. with PDCP SN from 0 to 100,000). 2. Bearer is moved to gNB as SCG split bearer there it continues PDCP SN (e.g. from 100,001 to 200,000). 3. Bearer is moved via full config to another gNB and stays SCG split bearer. It gets new key which is uses e.g. for PDCP SN 0 to 50,000 (no issue as there is new key). 4. Then the bearer is taken back to eNB and assume that the eNB did not yet have a key refresh. So old key will be used for PDCP SN 50,000 to 100,000. - *this would be same cipher stream as in first bullet above, i.e. would break LTE security*. 5. MeNB needs to handle this case. For example to trigger MeNB PCell HO in case of split bearer take-back, instead of   “LCID change with same DRB ID”. |   It is a security risk when NW move the DRB back from SN to the orginal termination point(MN) and reuse the same combination of security key, PDCP COUNT and DRBid.  It is clarified that network implementations must take care to prevent the security risk. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified that the security risk is present during multiple termination point change for RLC-AM and RLC-UM bearers (importing the clarification agreed in R2-1816725).  **Impact analysis**  Impacted functionality: Termination point change for RLC AM and RLC UM bearers.  Impacted architectures: EN-DC, NGEN-DC, NE-DC  Inter-operability: None. The changes impact network implementation only and hence no interoperability issues is foreseen. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The reuse of the same combination of security key, PDCP COUNT and DRB ID causes a and violates SA3 requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TS 38.331 CR 1539 | | |
| ***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 Modified Subclause*

#### 5.3.1.2 Security

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

RRC handles the configuration of the security parameters which are part of the AS configuration: the integrity protection algorithm, the ciphering algorithm and two parameters, namely the *keyChangeIndicator* and the *nextHopChainingCount,* which are used by the UE to determine the AS security keys upon handover, connection re-establishment, connection resume and/ or UP-EDT.

The integrity protection algorithm is common for signalling radio bearers SRB1, SRB2 and SRB4. When configured with MCG only, the ciphering algorithm is common for all radio bearers (i.e. SRB1, SRB2, SRB4 and DRBs). Neither integrity protection nor ciphering applies for SRB0.

RRC integrity and ciphering are always activated together, i.e. in one message/ procedure. RRC integrity and ciphering are never de-activated. However, it is possible to switch to a 'NULL' ciphering algorithm (eea0).

The 'NULL' integrity protection algorithm (eia0) is used only for the UE in limited service mode, as specified in TS 33.401 [32]. 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 check has failed and indicate the integrity verification check failure to RRC.

The AS applies three different security keys: one for the integrity protection of RRC signalling (KRRCint), one for the ciphering of RRC signalling (KRRCenc) and one for the ciphering of user data (KUPenc). All three AS keys are derived from the KeNB key. The KeNB is based on the KASME key for E-UTRA/EPC, or KAMF for E-UTRA/5GC, which is handled by upper layers.

Upon connection establishment new AS keys are derived. No AS-parameters are exchanged to serve as inputs for the derivation of the new AS keys at connection establishment.

The integrity and ciphering of the RRC message used to perform handover is based on the security configuration used prior to the handover and is performed by the source eNB.

The integrity and ciphering algorithms can only be changed upon handover. The four AS keys (KeNB, KRRCint, KRRCenc and KUPenc) change upon every handover, connection re-establishment, connection resume and UP-EDT. The *keyChangeIndicator* is used upon handover and indicates whether the UE should use the keys associated with the KASME key for E-UTRA/EPC, or KAMF for E-UTRA/5GC, taken into use with the latest successful NAS SMC procedure. The *nextHopChainingCount* parameter is used upon handover, connection re-establishment, connection resume and UP-EDT by the UE when deriving the new KeNB that is used to generate KRRCint, KRRCenc and KUPenc (see TS 33.401 [32]). An intra cell handover procedure may be used to change the keys in RRC\_CONNECTED.

For each radio bearer an independent counter (COUNT, as specified in TS 36.323 [8] for E-UTRA/EPC, and TS 38.323 [83] for E-UTRA/5GC) is maintained for each direction. For each DRB, the COUNT is used as input for ciphering. For each SRB, the COUNT is used as input for both ciphering and integrity protection. It is not allowed to use the same COUNT value more than once for a given security key. At connection resume the COUNT is reset. In order to limit the signalling overhead, individual messages/ packets include a short sequence number (PDCP SN, as specified in TS 36.323 [8] for E-UTRA/EPC, and TS 38.323 [83] for E-UTRA/5GC). In addition, an overflow counter mechanism is used: the hyper frame number (TX\_HFN and RX\_HFN, as specified in TS 36.323 [8] for E-UTRA/EPC, and TS 38.323 [83] for E-UTRA/5GC). The HFN needs to be synchronized between the UE and the eNB. The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same KeNB, 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, multiple termination point changes for RLC-AM bearer with SN terminated PDCP re-establishment (COUNT reset) due to SN only full configuration whilst the key stream inputs (i.e. bearer ID, security key) at MN have not been updated. In order to avoid such re-use, the eNB may e.g. use different RB identities for successive RB establishments, trigger an intra cell handover or by triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED.

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.

With E-UTRA/5GC for a UE not capable of NGEN-DC, the same ciphering algorithm signalled at SMC or handover is used for all radio bearers. Likewise, the same integrity algorithm signalled at SMC or handover is used for all SRBs.

In case of DC, a separate KeNB is used for SCG-DRBs (S-KeNB). This key is derived from the key used for the MCG (KeNB) and an SCG counter that is used to ensure freshness. To refresh the S-KeNB e.g. when the COUNT will wrap around, E-UTRAN employs an SCG change, i.e. an *RRCConnectionReconfiguration* message including *mobilityControlInfoSCG*. When performing handover, while at least one SCG-DRB remains configured, both KeNB and S-KeNB are refreshed. In such case E-UTRAN performs handover with SCG change i.e. an *RRCConnectionReconfiguration* message including both *mobilityControlInfo* and *mobilityControlInfoSCG*. The ciphering algorithm is common for all radio bearers within a CG but may be different between MCG and SCG. The ciphering algorithm for SCG DRBs can only be changed upon SCG change.

In case of (NG)EN-DC or of SN terminated RB without SCG, the network indicates whether the UE shall use either KeNB or S-KgNB for a particular DRB. In case of NE-DC, the network indicates whether the UE shall use either KgNB or S-KeNB for a particular DRB. S-KgNB/S-KeNB is derived from KeNB/KgNB as defined in TS 33.501 [86], uses a different counter (*sk-Counter*) and is used only for DRBs using NR PDCP. Whenever there is a need to refresh S-KgNB/S-KeNB, e.g. upon change of MN or SN, the NR SCG reconfiguration with sync and key change is used for S-KgNB refresh (see 5.3.1.1) and the *RRCConnectionReconfiguration* message including *mobilityControlInfoSCG* is used for S-KeNB refresh (see 5.3.10.10). E-UTRAN provides a UE configured with (NG)EN-DC with an *sk-Counter* even when no DRB is setup using S-KgNB i.e. to facilitate configuration of SRB3. The same ciphering algorithm as signalled by *nr-RadioBearerConfig1* and *nr-RadioBearerConfig2* as defined in TS 38.331 [82] is used for all radio bearers using the same key (i.e. KeNB or S-KgNB). Likewise, the same integrity algorithm as signalled by *nr-RadioBearerConfig1* and *nr-RadioBearerConfig2* as defined in TS 38.331 [82] is used for all SRBs using the same key. Although NR RRC uses different values for the security algorithms than E-UTRA, the actual algorithms are the same in case of (NG)EN-DC and NE-DC in this version of the specification. Hence, for such algorithms, the security capabilities supported by a UE are consistent across these RATs. For MR-DC, integrity protection is not enabled for DRBs terminated on eNB or when the master node is an ng-eNB.

NOTE 2: The network ensures that different values are used for the SCG counter and for the *sk-Counter* when deriving S-KgNB and/or S-KeNB from the same master key.

*End of changes*