**3GPP TSG-RAN2 Meeting #117 electronic *R2-2203821***

**Online, 21 Feb – 03 Mar, 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **36.300** | **CR** | **1353** | **rev** | **1** | **Current version:** | **16.7.0** |  |
|  |
| *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 | **X** | Radio Access Network | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Introducing support of UP IP for EPC connected architectures using NR PDCP |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, Vodafone, Ericsson, Qualcomm, Intel |
| ***Source to TSG:*** | RAN2 |
|  |  |
| ***Work item code:*** | UPIP\_SEC\_LTE-RAN-Core |  | ***Date:*** | 2022-03-10 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *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 canbe 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | In RP #94 meeting, User Plane Integrity Protection for EPC connected architectures using NR PDCP (i.e. UP IP applies to EN-DC capable UEs) was agreed to be supported in Rel-17 as in RP-213669. |
|  |  |
| ***Summary of change:*** | * In clause 14, adding descriptions that KUPint shall be derived for UEs capable of UP IP and UP IP can be activated/configured upon DRB addition with NR PDCP.

Note: In Table 14.2-1, the sentence of *Integrity protection for U-Plane is not required and thus it is not supported between UE and Serving Gateway or for the transport of user plane data between eNB and Serving Gateway on S1 interface* is in conflict with the description in TS 33.401 clause 5.3.4 (i.e. *The transport of user data over S1-U and X2-U shall be integrity, confidentially and replay-protected from unauthorized parties.*). It is agreed to correct the error by deleting the sentence. |
|  |  |
| ***Consequences if not approved:*** | UP IP can not be supported for LTE/EPC. |
|  |  |
| ***Clauses affected:*** | 14.1, 14.2, 14.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 36.331 CR #4763, TS 38.331 CR #2904, TS 37.340 CR #0294, TS 38.323 CR #0085 |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

14 Security

14.1 Overview and Principles

The following principles apply to E-UTRAN security:

- The keys used for NAS and AS protection shall be dependent on the algorithm with which they are used.

- The eNB keys are cryptographically separated from the EPC keys used for NAS protection (making it impossible to use the eNB key to figure out an EPC key).

- For SCG bearers in DC, the SeNB keys are cryptographically separated from the eNB keys.

- The AS (RRC and UP) and NAS keys are derived in the EPC/UE from key material that was generated by a NAS (EPC/UE) level AKA procedure (KASME) and identified with a key identifier (KSIASME).

- For SCG bearers in DC, the AS (UP) keys are derived in the SeNB/UE from key material that was generated in the MeNB/UE.

- The eNB key (KeNB) is sent from the EPC to the eNB when the UE is entering ECM-CONNECTED state (i.e. during RRC connection or S1 context setup).

- For SCG bearers in DC, the SeNB key (S-KeNB) is sent from the MeNB to the SeNB when adding an SCG.

- For LWA bearers, the WT Counter, if included in LWA Configuration, is used when computing the S-KWT (as specified in TS 33.401 [22], clause G and TS 36.331 [16], clause 5.6.14.2). If WT Counter is not signalled to the UE, the UE uses authentication methods specified in TS 33.402 [70], clause 6, as described in 22A.1.8.

- For LWIP, the LWIP Counter in the LWIP Configuration is used when computing the LWIP-PSK (as specified in TS 33.401 [13], clause A.13, and TS 36.331 [16], subcause 5.6.17.2).

- Separate AS and NAS level security mode command procedures are used. AS level security mode command procedure configures AS security (RRC and user plane) and NAS level security mode command procedure configures NAS security. Both integrity protection and ciphering for RRC are activated within the same AS SMC procedure. User plane ciphering is activated at the same time as RRC ciphering. An EN-DC capable UE supporting user plane integrity protection (see TS 24.301 [20]) when connected to E-UTRA/EPC (as specified in TS 33.401 [22]) shall support integrity protection for all DRBs (MN and SN terminated) at any data rate, up to and including the highest data rate supported by the UE for both UL and DL. When supported, user plane integrity protection with NR PDCP can be activated (on a per radio bearer basis) upon DRB addition.

- Keys stored inside eNBs shall never leave a secure environment within the eNB (except when done in accordance with this or other 3GPP specifications), and user plane data ciphering/deciphering shall take place inside the secure environment where the related keys are stored.

- Key material for the eNB keys is sent between the eNBs during ECM-CONNECTED intra-E-UTRAN mobility and from the MeNB to the SeNB in DC for SCG bearer during SCG addition and SCG change.

- A sequence number (COUNT) is used as input to the ciphering and integrity protection. A given sequence number must only be used once for a given eNB key (except for identical re-transmission) on the same radio bearer in the same direction. The same sequence number can be used for both ciphering and integrity protection.

- A hyper frame number (HFN) (i.e. an overflow counter mechanism) is used in the eNB and UE in order to limit the actual number of sequence number bits that is needed to be sent over the radio. The HFN needs to be synchronized between the UE and eNB.

- No integrity protection initialisation number (FRESH).

- Since SIM access is not granted in E-UTRAN TS 33.401 [22] except for making IMS Emergency calls, idle mode UE not equipped with USIM shall not attempt to reselect to E-UTRAN unless it is originating an IMS Emergency call. The RNC may try to prevent handover to E-UTRAN for example by identifying a SIM based UE from the security keys provided by the CN.

A simplified key derivation is depicted on Figure 14.1-1 below, where:

**- KNASint** is a key, which shall only be used for the protection of NAS traffic with a particular integrity algorithm This key is derived by UE and MME from KASME , as well as an identifier for the integrity algorithm.

**- KNASenc** is a key, which shall only be used for the protection of NAS traffic with a particular encryption algorithm. This key is derived by UE and MME from KASME, as well as an identifier for the encryption algorithm.

**- KeNB**is a key derived by UE and MME from KASME. KeNB may also be derived by the target eNB from NH at handover. KeNB shall be used for the derivation of KRRCint, KRRCenc and KUPenc, and for the derivation of KeNB**\*** upon handover.

- **KeNB\*** is a key derived by UE and source eNB from either KeNB or from a fresh NH. KeNB\* shall be used by UE and target eNB as a new KeNB for RRC and UP traffic.

- KUPint is a key, which shall only be used for the protection of UP traffic with a particular integrity algorithm. This key is derived by UE and eNB from KeNB, as well as an identifier for the integrity algorithm.

**- KUPenc**is a key, which shall only be used for the protection of UP traffic with a particular encryption algorithm. This key is derived by UE and eNB from KeNB, as well as an identifier for the encryption algorithm.

**- KRRCint** is a key, which shall only be used for the protection of RRC traffic with a particular integrity algorithm.KRRCint is derived by UE and eNB from KeNB, as well as an identifier for the integrity algorithm.

**- KRRCenc** is a key, which shall only be used for the protection of RRC traffic with a particular encryption algorithm.KRRCenc is derived by UE and eNB from KeNB as well as an identifier for the encryption algorithm.

- Next Hop (**NH**) is used by UE and eNB in the derivation of KeNB\* for the provision of "forward security", as specified in TS 33.401 [22]. NH is derived by UE and MME from KASME and KeNB when the security context is established, or from KASME and previous NH, otherwise.

- Next Hop Chaining Count (**NCC**) is a counter related to NH (i.e. the amount of Key chaining that has been performed) which allow the UE to be synchronised with the eNB and to determine whether the next **KeNB\*** needs to be based on the current KeNB or a fresh NH.



**Figure 14.1-1: Key Derivation**

Key derivation for SCG bearers in DC is depicted on Figure 14.1-2 below, where:

- SCG Counter is a counter used as freshness input into S-KeNB derivations (see TS 33.401 [22], Annex E.2.4).

****

**Figure 14.1-2: DC Key Derivation**

The MME invokes the AKA procedures by requesting authentication vectors to the HE (Home environment) if no unused EPS authentication vectors have been stored. The HE sends an authentication response back to the MME that contains a fresh authentication vector, including a base-key named KASME. Thus, as a result of an AKA run, the EPC and the UE share KASME. From KASME, the NAS keys, (and indirectly) KeNB keys and NH are derived. The KASME is never transported to an entity outside of the EPC, but KeNB and NH are transported to the eNB from the EPC when the UE transitions to ECM-CONNECTED. From the KeNB, the eNB and UE can derive the UP and RRC keys.

RRC and UP keys are refreshed at handover. KeNB\* is derived by UE and source eNB from target PCI, target frequency and KeNB (this is referred to as a *horizontal* key derivation and is indicated to UE with an NCC that does not increase) or from target PCI, target frequency and NH (this is referred to as a *vertical* key derivation and is indicated to UE with an NCC increase). KeNB\* is then used as new KeNB for RRC and UP traffic at the target. When the UE goes into ECM-IDLE all keys are deleted from the eNB except for the UE which was enabled to use User Plane CIoT EPS Optimisation.

For SCG Bearers in DC, UP keys are updated at SCG change by indicating in RRC signalling to the UE the value of the SCG Counter to be used in key derivation. When KeNB is refreshed, SCG Counter shall be reset and S-KeNB shall be newly derived from the KeNB.

COUNT reusing avoidance for the same radio bearer identity in RRC\_CONNECTED mode without KeNB change is left to eNB implementation e.g. by using intra-cell handover, smart management of radio bearer identities or triggering a transition to RRC\_IDLE.

SCG bearers in DC share a common pool of radio bearer identities (DRB IDs) together with the MCG bearers and when no new DRB ID can be allocated for an SCG bearer without guaranteeing COUNT reuse avoidance, the MeNB shall derive a new S-KeNB. SeNB indicates to MeNB when uplink or downlink PDCP COUNTs are about to wrap around and MeNB shall update the S-KeNB. To update the S-KeNB, the MeNB increases the SCG Counter and uses it to derive a new S-KeNB from the currently active KeNB in the MeNB. The MeNB sends the newly derived S-KeNB to the SeNB. The newly derived S-KeNB is then used by the SeNB in computing a new encryption key KUPenc which is used with all DRBs in the SeNB for this UE. Furthermore, when the SCG Counter approaches its maximum value, the MeNB refreshes the currently active KeNB, before any further S-KeNB is derived.

In case of HFN de-synchronisation in RRC\_CONNECTED mode between the UE and eNB, the UE is pushed to IDLE.

14.2 Security termination points

The table below describes the security termination points.

**Table 14.2-1 Security Termination Points**

|  |  |  |
| --- | --- | --- |
|  | **Ciphering** | **Integrity Protection** |
| NAS Signalling | Required and terminated in MME | Required and terminated in MME |
| U-Plane Data | Required and terminated in eNB  | Terminated in eNB(NOTE 1) |
| RRC Signalling (AS) | Required and terminated in eNB | Required and terminated in eNB |
| MAC Signalling (AS) | Not required | Not required |
| NOTE 1: User Plane Integrity Protection may be supported by UEs capable of EN-DC operation. This version of the specifications does not provide UPIP support for other UEs when using E-UTRA. |

The table below describes the security termination points for DC with SCG bearers and split bearers.

**Table 14.2-2 Security Termination Points in DC**

|  |  |  |
| --- | --- | --- |
|  | **Ciphering** | **Integrity Protection** |
| NAS Signalling | Required and terminated in MME | Required and terminated in MME |
| U-Plane Data for MCG bearers | Required and terminated in MeNB | Not Required |
| U-Plane Data for SCG bearers | Required and terminated in SeNB | Not Required |
| U-Plane Data for split bearers | Required and terminated in MeNB | Not Required |
| RRC Signalling (AS) | Required and terminated in MeNB | Required and terminated in MeNB |

Next change

14.4 AS Key Change in RRC\_CONNECTED

If AS Keys (KUPenc , KRRCint, KRRCenc and KUPint) need to be changed in RRC\_CONNECTED, an intra-cell handover shall be used.

For SCG bearers in DC, if AS Key (KUPenc) needs to be changed, the SCG change shall be performed.