**3GPP TSG-RAN2 Meeting #117 electronic *R2-220xxxx***

**Online, 21 Feb – 03 Mar, 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **36.331** | **CR** | **4763** | **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 |
| ***Source to TSG:*** | RAN2 |
|  |  |
| ***Work item code:*** | UPIP\_EN-DC\_UE |  | ***Date:*** | 2022-02-21 |
|  |  |  |  |  |
| ***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:*** | * Adding descriptions that KUPint shall be derived by UEs capable of UP IP upon reception of SMC or during HO.
 |
|  |  |
| ***Consequences if not approved:*** | UP IP can not be supported for LTE/EPC. |
|  |  |
| ***Clauses affected:*** | 5.3.1.2, 5.3.4.3, 5.3.5.4, 5.4.2.3, 6.3.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS 38.331 CR #2904, TS 36.300 CR #1353, 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:*** |  |

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, UP-EDT and/ or UP transmission using PUR.

The integrity protection algorithm is common for signalling radio bearers SRB1, SRB2, SRB4 if configured and DRBs configured with integrity protection. 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 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). For the UE capable of user plane integrity protection when it is connected to E-UTRA/EPC (TS 24.301 [35]), the AS also applies another security key for integrity protection of user data (KUPint) for the DRBs that are configured to apply integrity protection of user data. All 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 AS keys (KeNB, KRRCint, KRRCenc, KUPenc and KUPint ) change upon every handover, connection re-establishment, connection resume, UP-EDT and UP transmission using PUR. 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, UP-EDT and UP transmission using PUR 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. As specified in TS 33.401 subclause 7.2.9.1 [32], 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.

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 *HFN* as specified in TS 38.323 [83] for E-UTRA/5GC). The HFN needs to be synchronized between the UE and the eNB.

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 and DRBs configured to apply integrity protection of user data, 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 with 5GC, integrity protection is not enabled for DRBs terminated on ng-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.

Next change

5.3.4.3 Reception of the *SecurityModeCommand* by the UE

The UE shall:

1> derive the KeNB key, as specified in TS 33.401 [32] for E-UTRA/EPC, and TS 33.501 [86] for E-UTRA/5GC;

1> derive the KRRCint key associated with the *integrityProtAlgorithm* indicated in the *SecurityModeCommand* message, as specified in TS 33.401 [32];

1> request lower layers to verify the integrity protection of the *SecurityModeCommand* message, using the algorithm indicated by the *integrityProtAlgorithm* as included in the *SecurityModeCommand* message and the KRRCint key;

1> if the *SecurityModeCommand* message passes the integrity protection check:

2> derive the KRRCenc key and the KUPenc key associated with the *cipheringAlgorithm* indicated in the *SecurityModeCommand* message, as specified in TS 33.401 [32];

2> if connected as an RN; or

2> if capable of user plane integrity protection:

3> derive the KUPint key associated with the *integrityProtAlgorithm* indicated in the *SecurityModeCommand* message, as specified in TS 33.401 [32];

2> configure lower layers to apply integrity protection using the indicated algorithm and the KRRCint key immediately, i.e. integrity protection shall be applied to all subsequent messages received and sent by the UE, including the *SecurityModeComplete* message;

2> configure lower layers to apply ciphering using the indicated algorithm, the KRRCenc key and the KUPenc key after completing the procedure, i.e. ciphering shall be applied to all subsequent messages received and sent by the UE, except for the *SecurityModeComplete* message which is sent unciphered;

2> if connected as an RN:

3> configure lower layers to apply integrity protection using the indicated algorithm and the KUPint key, for DRBs that are subsequently configured to apply integrity protection, if any;

2> consider AS security to be activated;

2> upon RRC connection establishment, if UE does not need UL gaps during continuous uplink transmission:

3> configure lower layers to stop using UL gaps during continuous uplink transmission in FDD for *SecurityModeComplete* message and subsequent uplink transmission in RRC\_CONNECTED except for UL transmissions as specified in TS 36.211 [21];

2> submit the *SecurityModeComplete* message to lower layers for transmission, upon which the procedure ends;

1> else:

2> continue using the configuration used prior to the reception of the *SecurityModeCommand* message, i.e. neither apply integrity protection nor ciphering.

2> submit the *SecurityModeFailure* message to lower layers for transmission, upon which the procedure ends;

Next change

5.3.5.4 Reception of an *RRCConnectionReconfiguration* including the *mobilityControlInfo* by the UE (handover)

If the *RRCConnectionReconfiguration* message includes the *mobilityControlInfo* and theUE is able to comply with the configuration included in this message, the UE shall:

1> if *daps-HO* is not configured for any DRB:

2> stop timer T310, if running;

2> if timer T316 is running:

3> stop timer T316;

3> clear the information included in *VarRLF-Report*, if any;

2> resume MCG transmission, if suspended;

1> stop timer T312, if running;

1> start timer T304 with the timer value set to *t304,* as included in the *mobilityControlInfo*;

1> stop timer T370, if running;

1> if the *carrierFreq* is included:

2> consider the target PCell to be one on the frequency indicated by the *carrierFreq* with a physical cell identity indicated by the *targetPhysCellId*;

1> else:

2> consider the target PCell to be one on the frequency of the source PCell with a physical cell identity indicated by the *targetPhysCellId*;

1> if T309 is running:

2> stop timer T309 for all access categories;

2> perform the actions as specified in 5.3.16.4.

1> start synchronising to the DL of the target PCell;

NOTE 1: The UE should perform the handover as soon as possible following the reception of the RRC message triggering the handover, which could be before confirming successful reception (HARQ and ARQ) of this message.

1> if BL UE or UE in CE:

2> if *sameSFN-Indication* is not present in *mobilityControlInfo*:

3> acquire the *MasterInformationBlock* in the target PCell;

1> if *makeBeforeBreak* is configured:

2> perform the remainder of this procedure including and following resetting MAC after the UE has stopped the uplink transmission/downlink reception with the source PCell;

NOTE 1a: It is up to UE implementation when to stop the uplink transmission/ downlink reception with the source PCell to initiate re-tuning for connection to the target cell, as specified in TS 36.133 [16], if *makeBeforeBreak* is configured.

NOTE 1b: It is up to UE implementation when to stop the uplink transmission/ downlink reception with the source SCell(s) after receiving *RRCConnectionReconfiguration* message.

1> if *daps-HO* is configured for any DRB:

2> establish a MAC entity for the target PCell, with the same configuration as the MAC entity for the source PCell;

2> for each DRB configured with *daps-HO*:

3> establish the RLC entity or entities and the associated DTCH logical channel for the target PCell, with the same configurations as for the source PCell;

3> reconfigure the PDCP entity to configure DAPS as specified in TS36.323 [8].

2> for each DRB not configured with *daps-HO*:

3> re-establish PDCP;

3> re-establish the RLC entity and associate it, and the associated DTCH logical channel, to the target PCell;

2> for each SRB:

3> establish a PDCP entity for the target PCell, with the same configuration as the PDCP entity for the source PCell;

3> establish an RLC entity and an associated DCCH logical channel for the target PCell, with the same configuration as for the source PCell;

2> suspend the SRBs for the source PCell;

NOTE 1c: In order to understand if a *daps-HO* is configured, the UE needs to check the presence of the field *daps-HO* within the received *RadioResourceConfigDedicated* IE.

NOTE 1d: In DAPS handover, the UE may re-establish PDCP and RLC entity for a DRB not configured with *daps-HO* when MAC successfully completes the random access procedure. In this case, the UE suspends data transmission and reception for all DRBs not configured with *daps-HO* in the source PCell for the duration of the DAPS handover.

1> else (if *daps-HO* is not configured):

2> reset MCG MAC and SCG MAC, if configured;

2> release *uplinkDataCompression*, if configured;

2> re-establish PDCP for all RBs configured with *pdcp-config* that are established;

NOTE 2: The handling of the radio bearers after the successful completion of the PDCP re-establishment, e.g. the re-transmission of unacknowledged PDCP SDUs (as well as the associated status reporting), the handling of the SN and the HFN, is specified in TS 36.323 [8].

NOTE 2a: At handover the *reestablishPDCP* flag will be set for all RBs configured with NR PDCP in *nr-RadioBearerConfig1* or *nr-RadioBearerConfig2* TS 38.331 [82] which will cause the PDCP entity to be re-established also for these RBs.

2> re-establish MCG RLC and SCG RLC, if configured, for all RBs that are established;

1> for each SCell configured for the UE other than the PSCell:

2> if the received *RRCConnectionReconfiguration* message includes *sCellState* for the SCell and indicates *activated*:

3> configure lower layers to consider the SCell to be in activated state;

2> else if the received *RRCConnectionReconfiguration* message includes *sCellState* for the SCell and indicates *dormant*:

3> configure lower layers to consider the SCell to be in dormant state;

2> else:

3> configure lower layers to consider the SCell to be in deactivated state;

1> apply the value of the *newUE-Identity* as the C-RNTI in the target MCG;

1> if the *RRCConnectionReconfiguration* message includes the *fullConfig*:

2> perform the radio configuration procedure as specified in 5.3.5.8;

1> configure lower layers in accordance with the received *radioResourceConfigCommon*;

1> if the received *RRCConnectionReconfiguration* message includes the *rach-Skip*:

2> configure lower layers to apply the *rach-Skip* for the target MCG, as specified in TS 36.213 [23] and 36.321 [6];

1> configure lower layers in accordance with any additional fields, not covered in the previous, if included in the received mobilityControlInfo;

1> if the received *RRCConnectionReconfiguration* includes the *sCellToReleaseList*:

2> perform SCell release as specified in 5.3.10.3a;

1> if the received *RRCConnectionReconfiguration* includes the *sCellGroupToReleaseList*:

2> perform SCell group release as specified in 5.3.10.3d;

1> if the received *RRCConnectionReconfiguration* includes the *scg-Configuration*; or

1> if the current UE configuration includes one or more split DRBs and the received *RRCConnectionReconfiguration* includes *radioResourceConfigDedicated* including *drb-ToAddModList*:

2> perform SCG reconfiguration as specified in 5.3.10.10;

1> if the *RRCConnectionReconfiguration* message includes the *radioResourceConfigDedicated*:

2> perform the radio resource configuration procedure as specified in 5.3.10;

1> if the *securityConfigHO* (without suffix) is included in the *RRCConnectionReconfiguration*:

2> if the *keyChangeIndicator* received in the *securityConfigHO* is set to *TRUE*:

3> update the KeNB key based on the KASME key taken into use with the latest successful NAS SMC procedure, as specified in TS 33.401 [32];

2> else:

3> update the KeNB key based on the current KeNB or the NH, using the *nextHopChainingCount* value indicated in the *securityConfigHO*, as specified in TS 33.401 [32];

NOTE 2b: If the UE needs to update the S-KeNB key as specified in 5.3.10.10, the UE updates the S-KeNB after updating the KeNB key.

2> store the *nextHopChainingCount* value;

2> if the *securityAlgorithmConfig* is included in the *securityConfigHO*:

3> derive the KRRCint key associated with the *integrityProtAlgorithm*, as specified in TS 33.401 [32];

3> if connected as an RN, or:

3> if capable of user plane integrity protection:

4> derive the KUPint key associated with the *integrityProtAlgorithm*, as specified in TS 33.401 [32];

3> derive the KRRCenc key and the KUPenc key associated with the *cipheringAlgorithm*, as specified in TS 33.401 [32];

2> else:

3> derive the KRRCint key associated with the current integrity algorithm, as specified in TS 33.401 [32];

3> if connected as an RN:

4> derive the KUPint key associated with the current integrity algorithm, as specified in TS 33.401 [32];

3> derive the KRRCenc key and the KUPenc key associated with the current ciphering algorithm, as specified in TS 33.401 [32];

2> configure lower layers to apply the integrity protection algorithm and the KRRCint key, i.e. the integrity protection configuration shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

2> configure lower layers to apply the ciphering algorithm, the KRRCenc key and the KUPenc key, i.e. the ciphering configuration shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

NOTE 2c: For a DRB configured for DAPS HO, the new ciphering algorithm and the KUPenc key is applied for traffic exchange between the UE and the target MCG while the old ciphering algorithm and KUPenc key is applied for traffic exchange between the UE and the source MCG.

1> else if the *securityConfigHO-v1530* is included in the *RRCConnectionReconfiguration*:

2> if the *nas-Container* is received:

3> forward the *nas-Container* to upper layers;

2> if the *keyChangeIndicator-r15* is received and is set to *TRUE*:

3> update the KeNB key based on the KAMF key, as specified in TS 33.501 [86];

2> else:

3> update the KeNB key based on the current KeNB or the NH, using the received *nextHopChainingCount-r15*, as specified in TS 33.501 [86];

2> store the *nextHopChainingCount-r15* value;

2> if the security*AlgorithmConfig-r15* is received:

3> derive the KRRCint key associated with the *integrityProtAlgorithm*, as specified in TS 33.401 [32];

3> derive the KRRCenc key and the KUPenc key associated with the *cipheringAlgorithm*, as specified in TS 33.401 [32];

2> else:

3> derive the KRRCint key associated with the current integrity algorithm, as specified in TS 33.401 [32];

3> derive the KRRCenc key and the KUPenc key associated with the current ciphering algorithm, as specified in TS 33.401 [32];

1> if the received *RRCConnectionReconfiguration* includes the *nr-Config* and it is set to *release*; or

1> if the received *RRCConnectionReconfiguration* includes *endc-ReleaseAndAdd* and it is set to *TRUE*:

2> perform MR-DC release as specified in TS 38.331 [82], clause 5.3.5.10;

1> if the received *RRCConnectionReconfiguration* includes the *sk-Counter*:

2> perform key update procedure as specified in in TS 38.331 [82], clause 5.3.5.7;

1> if the received *RRCConnectionReconfiguration* includes the *nr-SecondaryCellGroupConfig*:

2> perform NR RRC Reconfiguration as specified in TS 38.331 [82], clause 5.3.5.3.

1> if the received *RRCConnectionReconfiguration* includes the *nr-RadioBearerConfig1*:

2> perform radio bearer configuration as specified in TS 38.331 [82], clause 5.3.5.6;

1> if the received *RRCConnectionReconfiguration* includes the *nr-RadioBearerConfig2*:

2> perform radio bearer configuration as specified in TS 38.331 [82], clause 5.3.5.6.

1> if connected as an RN:

2> configure lower layers to apply the integrity protection algorithm and the KUPint key, for current or subsequently established DRBs that are configured to apply integrity protection, if any;

1> if the received *RRCConnectionReconfiguration* includes the *sCellToAddModList*:

2> perform SCell addition or modification as specified in 5.3.10.3b;

1> if the received *RRCConnectionReconfiguration* includes the *sCellGroupToAddModList*:

2> perform SCell group addition or modification as specified in 5.3.10.3e;

1> if the received *RRCConnectionReconfiguration* includes the *systemInformationBlockType1Dedicated*:

2> perfom the actions upon reception of the *SystemInformationBlockType1* message as specified in 5.2.2.7;

1> perform the measurement related actions as specified in 5.5.6.1;

1> if the *RRCConnectionReconfiguration* message includes the *measConfig*:

2> perform the measurement configuration procedure as specified in 5.5.2;

1> perform the measurement identity autonomous removal as specified in 5.5.2.2a;

1> release *reportProximityConfig* and clear any associated proximity status reporting timer;

1> if the *RRCConnectionReconfiguration* message includes the *otherConfig*:

2> perform the other configuration procedure as specified in 5.3.10.9;

1> if the *RRCConnectionReconfiguration* message includes the *sl-DiscConfig* or *sl-CommConfig*:

2> perform the sidelink dedicated configuration procedure as specified in 5.3.10.15;

1> if the *RRCConnectionReconfiguration* message includes *wlan-OffloadInfo*:

2> perform the dedicated WLAN offload configuration procedure as specified in 5.6.12.2;

1> if *handoverWithoutWT-Change* is not configured:

2> release the LWA configuration, if configured, as described in 5.6.14.3;

1> release the LWIP configuration, if configured, as described in 5.6.17.3;

1> if the *RRCConnectionReconfiguration* message includes *rclwi-Configuration*:

2> perform the WLAN traffic steering command procedure as specified in 5.6.16.2;

1> if the *RRCConnectionReconfiguration* message includes *lwa-Configuration*:

2> perform the LWA configuration procedure as specified in 5.6.14.2;

1> if the *RRCConnectionReconfiguration* message includes *lwip-Configuration*:

2> perform the LWIP reconfiguration procedure as specified in 5.6.17.2;

1> if the *RRCConnectionReconfiguration* message includes the *sl-V2X-ConfigDedicated* or *mobilityControlInfoV2X*:

2> perform the V2X sidelink communication dedicated configuration procedure as specified in 5.3.10.15a;

NOTE 2d: In case of conditional reconfiguration the text "if the received *RRCConnectionReconfiguration. . .*" corresponds to applying the stored *RRCConnectionReconfiguration* message (according to 5.3.5.9.5).

1> if the UE is configured to operate in EN-DC as result of this procedure, forward *upperLayerIndication*, as if the UE receives this field from SIB2, to upper layers, otherwise indicate upper layers absence of this field;

1> set the content of *RRCConnectionReconfigurationComplete* message as follows:

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report*:

3> include *rlf-InfoAvailable*;

2> if the UE has MBSFN logged measurements available for E-UTRA and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport* and if T330 is not running:

3> include *logMeasAvailableMBSFN*;

2> else if the UE has logged measurements available for E-UTRA and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport*:

3> include the *logMeasAvailable*;

3> if Bluetooth measurement results are included in the logged measurements the UE has available:

4> include *logMeasAvailableBT*;

3> if WLAN measurement results are included in the logged measurements the UE has available:

4> include *logMeasAvailableWLAN*;

2> if the UE has connection establishment failure information available in *VarConnEstFailReport* and if the RPLMN is equal to *plmn-Identity* stored in *VarConnEstFailReport*:

3> include *connEstFailInfoAvailable*;

2> if the *RRCConnectionReconfiguration* message includes *perCC-GapIndicationRequest*:

3> include *perCC-GapIndicationList* and *numFreqEffective*;

2> if the frequencies are configured for reduced measurement performance:

3> include *numFreqEffectiveReduced*;

2> if the UE has flight path information available:

3> include *flightPathInfoAvailable*;

2> if the received *RRCConnectionReconfiguration* message included *nr-SecondaryCellGroupConfig*:

3> include *scg-ConfigResponseNR* in accordance with TS 38.331 [82], clause 5.3.5.3;

1> submit the *RRCConnectionReconfigurationComplete* message to lower layers for transmission;

1> if MAC successfully completes the random access procedure; or

1> if MAC indicates the successful reception of a PDCCH transmission addressed to C-RNTI and if *rach-Skip* is configured:

2> stop timer T304;

2> if *daps-HO* is configured for any DRB:

3> stop timer T310 for the source PCell, if running;

3> for each DAPS bearer trigger UL data switching, as specified in TS 36.323 [8];

2> release *rach-Skip*;

2> apply the parts of the CQI reporting configuration, the scheduling request configuration and the sounding RS configuration that do not require the UE to know the SFN of the target PCell, if any;

2> apply the parts of the measurement and the radio resource configuration that require the UE to know the SFN of the target PCell (e.g. measurement gaps, periodic CQI reporting, scheduling request configuration, sounding RS configuration), if any, upon acquiring the SFN of the target PCell;

NOTE 3: Whenever the UE shall setup or reconfigure a configuration in accordance with a field that is received it applies the new configuration, except for the cases addressed by the above statements.

2> if the UE is configured to provide IDC indications:

3> if the UE has initiated the transmission of an *InDeviceCoexIndication* message during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

3> if the *RRCConnectionReconfiguration* message is applied due to a conditional reconfiguration execution and the UE has initiated transmission of an *InDeviceCoexIndication* message since it was configured to do so in accordance with 5.6.9.2:

4> initiate transmission of the *InDeviceCoexIndication* message in accordance with 5.6.9.3;

2> if the UE is configured to provide power preference indications, overheating assistance information, SPS assistance information, delay budget report or maximum bandwidth preference indications:

3> if the UE has initiated the transmission of a *UEAssistanceInformation* message during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

3> if the *RRCConnectionReconfiguration* message is applied due to a conditional reconfiguration execution, and the UE has initiated transmission of a *UEAssistanceInformation* message for the corresponding cell group since it was configured to do so in accordance with 5.6.10.2:

4> initiate transmission of the *UEAssistanceInformation* message in accordance with 5.6.10.3;

2> if *SystemInformationBlockType15* is broadcast by the PCell:

3> if the UE has initiated the transmission of a *MBMSInterestIndication* message during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

3> if the *RRCConnectionReconfiguration* message is applied due to a conditional reconfiguration execution and the UE supports MBMS reception and the UE has initiated transmission of an *MBMSInterestIndication* message since it was configured to do so in accordance with 5.8.5.2:

4> ensure having a valid version of *SystemInformationBlockType15* for the PCell;

4> determine the set of MBMS frequencies of interest in accordance with 5.8.5.3;

4> determine the set of MBMS services of interest in accordance with 5.8.5.3a;

4> initiate transmission of the *MBMSInterestIndication* message in accordance with 5.8.5.4;

2> if *SystemInformationBlockType18* is broadcast by the target PCell; and the UE initiated the transmission of a *SidelinkUEInformation* message indicating a change of sidelink communication related parameters relevant in target PCell (i.e. change of *commRxInterestedFreq* or *commTxResourceReq*, *commTxResourceReqUC* if *SystemInformationBlockType18* includes *commTxResourceUC-ReqAllowed* or *commTxResourceInfoReqRelay* if PCell broadcasts *SystemInformationBlockType19* including *discConfigRelay*) during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

2> if *SystemInformationBlockType19* is broadcast by the target PCell; and the UE initiated the transmission of a *SidelinkUEInformation* message indicating a change of sidelink discovery related parameters relevant in target PCell (i.e. change of *discRxInterest* or *discTxResourceReq*, *discTxResourceReqPS* if *SystemInformationBlockType19* includes *discConfigPS* or *discRxGapReq* or *discTxGapReq* if the UE is configured with *gapRequestsAllowedDedicated* set to *true* or if the UE is not configured with *gapRequestsAllowedDedicated* and *SystemInformationBlockType19* includes *gapRequestsAllowedCommon*) during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

2> if *SystemInformationBlockType21* is broadcast by the target PCell; and the UE initiated the transmission of a *SidelinkUEInformation* message indicating a change of V2X sidelink communication related parameters relevant in target PCell (i.e. change of *v2x-CommRxInterestedFreqList* or *v2x-CommTxResourceReq*) during the last 1 second preceding reception of the *RRCConnectionReconfiguration* message including *mobilityControlInfo*; or

2> if the *RRCConnectionReconfiguration* message is applied due to a conditional reconfiguration execution, and at least one of *SystemInformationBlockType18*, *SystemInformationBlockType19*, and *SystemInformationBlockType21* is broadcast by the target PCell, and the UE has initiated transmission of a *SidelinkUEInformation* message since it was configured to do so in accordance with 5.10.2.2:

3> initiate transmission of the *SidelinkUEInformation* message in accordance with 5.10.2.3;

2> remove all the entries within *VarConditionalReconfiguration*, if any;

2> for each *measId* of the source SpCell configuration, if the associated *reportConfig* is *condReconfigurationTriggerEUTRA*:

3> remove the entry with the matching *measId* from the *measIdList* within the *VarMeasConfig*;

3> remove the entry with the matching *reportConfigId* from the *reportConfigList* within the *VarMeasConfig*;

3> if the *measObjectId* is only included in a *MeasIdToAddMod*:

4> remove the entry with the matching *measObjectId* from the *measObjectList* within the *VarMeasConfig*;

2> the procedure ends;

NOTE 4: The UE is not required to determine the SFN of the target PCell by acquiring system information from that cell before performing RACH access in the target PCell, except for BL UEs or UEs in CE when *sameSFN-Indication* is not present in *mobilityControlInfo*.

Next change

5.4.2.3 Reception of the *RRCConnectionReconfiguration* by the UE

If the UE is able to comply with the configuration included in the *RRCConnectionReconfiguration* message, the UE shall:

1> if the *RRCConnectionReconfiguration* message does not include the *fullConfig* and the UE is connected to 5GC (i.e., delta signalling during intra 5GC handover):

2> re-use the source SDAP and PDCP configurations (i.e., current SDAP/PDCP configurations for all RBs from source RAT prior to the reception of the inter-RAT handover *RRCConnectionReconfiguration* message);

1> if the *RRCConnectionReconfiguration* message includes the *fullConfig* and the source RAT was E-UTRA (i.e., intra-RAT inter-system handover):

2> except the MCG C-RNTI, release/ clear all current dedicated radio resources and configurations, including all SDAP (if configured), PDCP, RLC, logical channel configurations for the DRBs and the logged measurement configuration (if configured);

2> release/ clear all current common radio configurations;

2> for each *srb-Identity* value included in the *srb-ToAddModList* (SRB reconfiguration):

3> apply the specified configuration defined in 9.1.2 for the corresponding SRB;

3> apply the corresponding default RLC configuration for the SRB specified in 9.2.1.1 for SRB1 or in 9.2.1.2 for SRB2;

3> apply the corresponding default logical channel configuration for the SRB as specified in 9.2.1.1 for SRB1 or in 9.2.1.2 for SRB2;

3> if the *handoverType* in *securityConfigHO* is set to *fivegc-ToEPC* (i.e, the UE is connecting to EPC):

4> release the PDCP entity and establish it with an E-UTRA PDCP entity;

3> else if the *handoverType* in *securityConfigHO* is set to *epc-To5GC* (i.e., the UE is connecting to 5GC):

4> release the PDCP entity and establish it with an NR PDCP and apply the corresponding default PDCP configuration for the SRB as specified in TS 38.331 [82], clause 9.2.1;

3> associate the RLC bearer of this SRB with the established PDCP entity;

1> apply the default physical channel configuration as specified in 9.2.4;

1> apply the default semi-persistent scheduling configuration as specified in 9.2.3;

1> apply the default MAC main configuration as specified in 9.2.2;

1> start timer T304 with the timer value set to *t304,* as included in the *mobilityControlInfo*;

1> consider the target PCell to be one on the frequency indicated by the *carrierFreq* with a physical cell identity indicated by the *targetPhysCellId*;

1> start synchronising to the DL of the target PCell;

1> set the C-RNTI to the value of the *newUE-Identity*;

1> for the target PCell, apply the downlink bandwidth indicated by the *dl-Bandwidth;*

1> for the target PCell, apply the uplink bandwidth indicated by (the absence or presence of) the *ul-Bandwidth;*

1> configure lower layers in accordance with the received *radioResourceConfigCommon*;

1> configure lower layers in accordance with any additional fields, not covered in the previous, if included in the received *mobilityControlInfo*;

1> perform the radio resource configuration procedure as specified in 5.3.10;

1> if the *handoverType* in *securityConfigHO* is set to *fivegc-ToEPC*:

2> indicate to higher layer that the CN has changed from 5GC to EPC;

2> derive the key KeNB based on the mapped KASME key as specified for interworking between EPS and 5GS in TS 33.501 [86];

2> store the *nextHopChainingCount-r15* value;

1> else if the *handoverType* in *securityConfigHO* is set to *intra5GC*:

2> if the *keyChangeIndicator-r15* received in the *securityConfigHO* is set to *TRUE*:

3> forward *nas-Container* to the upper layers, if included;

3> update the KeNB key based on the KAMF key, as specified in TS 33.501 [86];

2> else:

3> update the KeNB key based on the current KgNB or the NH, using the *nextHopChainingCount-r15* value indicated in the *SecurityConfigHO*, as specified in TS 33.501 [86];

2> store the *nextHopChainingCount-r15* value;

1> else if the *handoverType* in *securityConfigHO* is set to *epc-To5GC*:

2> forward the *nas-Container* to the upper layers

2> derive the KeNB key, as specified in TS 33.501 [86];

1> else:

2> forward the *nas-SecurityParamToEUTRA* to the upper layers;

2> derive the KeNB key, as specified in TS 33.401 [32];

1> derive the KRRCint key associated with the *integrityProtAlgorithm*, as specified in TS 33.401 [32];

1> derive the KRRCenc key and the KUPenc key associated with the *cipheringAlgorithm*, as specified in TS 33.401 [32];

1> if capable of user plane integrity protection:

2> derive the KUPint key associated with the integrityProtAlgorithm, as specified in TS 33.401 [32];

1> if the received *RRCConnectionReconfiguration* includes the *sk-Counter*:

2> perform key update procedure as specified in in TS 38.331 [82], clause 5.3.5.7;

1> if the received *RRCConnectionReconfiguration* includes the *nr-SecondaryCellGroupConfig*:

2> perform NR RRC Reconfiguration as specified in TS 38.331 [82], clause 5.3.5.3;

1> if the received *RRCConnectionReconfiguration* includes the *nr-RadioBearerConfig1*:

2> perform radio bearer configuration as specified in TS 38.331 [82], clause 5.3.5.6;

1> if the received *RRCConnectionReconfiguration* includes the *nr-RadioBearerConfig2*:

2> perform radio bearer configuration as specified in TS 38.331 [82], clause 5.3.5.6;

1> if the *handoverType* in *securityConfigHO* is set to *fivegc-ToEPC* orif the *handoverType-v1530* is not present:

2> configure lower layers to apply the indicated integrity protection algorithm and the KRRCint key immediately, i.e. the indicated integrity protection configuration shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

2> configure lower layers to apply the indicated ciphering algorithm, the KRRCenc key and the KUPenc key immediately, i.e. the indicated ciphering configuration shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

1> if the received *RRCConnectionReconfiguration* includes the s*CellToAddModList*:

2> perform SCell addition as specified in 5.3.10.3b;

1> if the *RRCConnectionReconfiguration* message includes the *measConfig*:

2> perform the measurement configuration procedure as specified in 5.5.2;

1> perform the measurement identity autonomous removal as specified in 5.5.2.2a;

1> if the *RRCConnectionReconfiguration* message includes the *otherConfig*:

2> perform the other configuration procedure as specified in 5.3.10.9;

1> if the *RRCConnectionReconfiguration* message includes *wlan-OffloadInfo*:

2> perform the dedicated WLAN offload configuration procedure as specified in 5.6.12.2;

1> if the *RRCConnectionReconfiguration* message includes *rclwi-Configuration*:

2> perform the WLAN traffic steering command procedure as specified in 5.6.16.2;

1> if the *RRCConnectionReconfiguration* message includes *lwa-Configuration*:

2> perform the LWA configuration procedure as specified in 5.6.14.2;

1> if the *RRCConnectionReconfiguration* message includes *lwip-Configuration*:

2> perform the LWIP reconfiguration procedure as specified in 5.6.17.2;

1> set the content of *RRCConnectionReconfigurationComplete* message as follows:

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report*:

3> include *rlf-InfoAvailable*;

2> if the UE has MBSFN logged measurements available for E-UTRA and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport* and if T330 is not running:

3> include *logMeasAvailableMBSFN*;

2> else if the UE has logged measurements available for E-UTRA and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport*:

3> include the *logMeasAvailable*;

3> if Bluetooth measurement results are included in the logged measurements the UE has available:

4> include the *logMeasAvailableBT*;

3> if WLAN measurement results are included in the logged measurements the UE has available:

4> include the *logMeasAvailableWLAN*;

2> if the UE has connection establishment failure information available in *VarConnEstFailReport* and if the RPLMN is equal to *plmn-Identity* stored in *VarConnEstFailReport*:

3> include *connEstFailInfoAvailable*;

2> if the received *RRCConnectionReconfiguration* message included *nr-SecondaryCellGroupConfig*:

3> include *scg-ConfigResponseNR* in accordance with TS 38.331 [82], clause 5.3.5.3;

1> submit the *RRCConnectionReconfigurationComplete* message to lower layers for transmission using the new configuration;

1> if the *RRCConnectionReconfiguration* message does not include *rlf-TimersAndConstants* set to *setup*:

2> use the default values specified in 9.2.5 for timer T310, T311 and constant N310, N311;

1> if MAC successfully completes the random access procedure:

2> stop timer T304;

2> apply the parts of the CQI reporting configuration, the scheduling request configuration and the sounding RS configuration that do not require the UE to know the SFN of the target PCell, if any;

2> apply the parts of the measurement and the radio resource configuration that require the UE to know the SFN of the target PCell (e.g. measurement gaps, periodic CQI reporting, scheduling request configuration, sounding RS configuration), if any, upon acquiring the SFN of the target PCell;

NOTE 1: Whenever the UE shall setup or reconfigure a configuration in accordance with a field that is received it applies the new configuration, except for the cases addressed by the above statements.

2> enter E-UTRA RRC\_CONNECTED, upon which the procedure ends;

NOTE 2: The UE is not required to determine the SFN of the target PCell by acquiring system information from that cell before performing RACH access in the target PCell.

NOTE 3: If the handover is from NR and target CN is 5GC, the delta configuration on PDCP and SDAP can be used for intra-system inter-RAT handover. For other cases, source RAT configuration is not considered when the UE applies the reconfiguration message of target RAT.

Next change

### 6.3.3 Security control information elements

– *SecurityAlgorithmConfig*

The IE *SecurityAlgorithmConfig* is used to configure AS integrity protection algorithm (SRBs) and AS ciphering algorithm (SRBs and DRBs). For RNs, the IE *SecurityAlgorithmConfig* is also used to configure AS integrity protection algorithm for DRBs between the RN and the E-UTRAN.

***SecurityAlgorithmConfig* information element**

-- ASN1START

SecurityAlgorithmConfig ::= SEQUENCE {

 cipheringAlgorithm CipheringAlgorithm-r12,

 integrityProtAlgorithm ENUMERATED {

 eia0-v920, eia1, eia2, eia3-v1130, spare4, spare3,

 spare2, spare1, ...}

}

CipheringAlgorithm-r12 ::= ENUMERATED {

 eea0, eea1, eea2, eea3-v1130, spare4, spare3,

 spare2, spare1, ...}

-- ASN1STOP

| ***SecurityAlgorithmConfig* field descriptions** |
| --- |
| ***cipheringAlgorithm***Indicates the ciphering algorithm to be used for SRBs and DRBs, as specified in TS 33.401 [32], clause 5.1.3.2. |
| ***integrityProtAlgorithm***Indicates the integrity protection algorithm to be used for SRBs, as specified in TS 33.401 [32], clause 5.1.4.2. For RNs and for UEs capable of user plane integrity protection, also indicates the integrity protection algorithm to be used for integrity protection-enabled DRB(s). |