**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212771-r1***

**e-meeting, 16 - 27 August 2021 merge with S3-212695**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.401** | **CR** | **DraftCR** | **rev** |  | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | User Plane Integrity Protection Policy Handling in EN-DC | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Huawei? | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPIP\_SEC\_LTE | | | | |  | ***Date:*** | | | 2021-08-09 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | UP IP policy handling and activation of UP IP in the SgNB in EN-DC is not specified yet | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add text for UP IP policy handling and activation of UP IP in the SgNB in EN-DC | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification is not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | E.1.3, E.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

E.1.3 Dual Connecivity architecture with an SgNB

Annex E.3 describes the security functions necessary to support a UE that is simultaneously connected to eNB as master and gNB as secondary for EN-DC dual connectivity. The description in Annex E.3 is focused on the difference from dual connectivity in E-UTRAN described in Annex E.2. The major differences are

a) with dual connectivity between an MeNB and an SgNB compared to between an MeNB and an SeNB is that in the former case a RRC signalling connection is allowed between the UE and the SgNB. Such a RRC signalling connection shall be integrity protected in addition to the ciphered with the chosen ciphering algorithm;

b) EPS bearers from the core network to the SgNB may be Split across the radio resources of both MeNB and SgNB (as well as being Non-Split and only using radio resources of the SgNB); and

c) for bearers whose PDCP terminates in the MeNB, the security functions described for the single connectivity mode in this specification shall be used, while for bearers whose PDCP terminates in the SgNB, the security algorithm given in subclause E.3.10.1 with key derived as given in clause A.19 shall be used.



**Figure E.1.3-1 Offload architecture for EN-DC**

When the MeNB establishes security between a SgNB and the UE for the first time for a given AS security context shared between the MeNB and the UE, the MeNB generates the S-KgNB (exactly as it would generate an S-KeNB) for the SgNB and sends it to the SgNB over the X2-C. The SCG Counter is also used as freshness input into S-KgNB derivations as described in the clause E.2.4, and guarantees, together with the other provisions in the present clause E, that the integrity and ciphering keys used at the SgNB derived from the same S-KgNB are not re-used with the same input parameters to avoid in key-stream re-use and provide replay protection. The MeNB sends the value of the SCG Counter to the UE over the LTE RRC signalling path when it is required to generate a new S-KgNB.

The communication established between the SgNB and the UE is protected at the PDCP layer using the SgNB Secondary Cell security context, or SgNB SC security context for short. The SgNB SC security context includes S-KgNB, the key used as input to the UP confidentiality algorithm, KSgNB-UP-enc, the key used as input to the UP integrity algorithm, KSgNB-UP-int, the key used as the input to the RRC confidentiality algorithm, KSgNB-RRC-enc, the key used as the input for the RRC integrity algorithm, KSgNB-RRC-int, the identifiers of the selected cryptographic algorithms and counters used for replay protection. The UE and the SgNB derives the integrity and ciphering keys from the S-KgNB as described in clause A.19, cf. also E.3.4.2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# E.3 Dual connectivity architecture between a MeNB and a SgNB

## E.3.1 Protection of the X2 reference point

The protection of X2 interface shall use the X2-C security and X2-U security as described in subclause E.2.1 of the present document.

## E.3.2 Addition and modification of DRBs and/or SRB in SgNB

The S-KeNB that is used for dual connectivity between eNBs (see subclause E.2.3) is also used as the root for the security context at the SgNB. When used in the contexts of dual connectivity with an SgNB, the key shall be called an S-KgNB, i.e. the MeNB generates and forwards an S-KgNB to the SgNB during the SgNB Addition procedure or SgNB Modification procedure requiring key update.

NOTE 1: Refer to TS 36.300 [30] for definition of the SgNB Addition and SgNB Modification procedures.

Similarly, the MeNB handles the SCG Counter due to interactions with a SgNB as described in subclause E.2.2 for interactions with SeNBs, i.e. this is a single shared SCG Counter for SeNBs and SgNBs and provides the same value of SCG Counter used to the UE and ensure that fresh radio bearer identities are used or the S-KgNB is refreshed.

When the SgNB receives an S-KgNB in a SgNB Addition/Modification procedure, the SgNB shall derive and store KSgNB-UP-enc and KSgNB-UP-int, as well as KSgNB-RRC-int and KSgNB-RRC-enc if an SRB is to be added as described in subclause E.3.4.2 from the received S-KgNB. These freshly derived keys are then used to protect all the radio bearer(s) that use the PDCP of the SgNB. Any previous such keys shall be deleted. If all the keys were derived, then the S-KgNB may be deleted.

NOTE 2: Void.

If the UE receives a new SCG Counter in SgNB Addition/Modification procedure, then the UE shall derive a new S-KgNB from this SCG Counter and use KSgNB-UP-enc, KSgNB-UP-int, KSgNB-RRC-int and KSgNB-RRC-enc derived from the new S-KgNB, as the keys to protect all the radio bearer(s) using the PDCP of the SgNB. If all the keys were derived, then the S-KgNB may be deleted in the UE.

When the SgNB Release procedure releases the last radio bearer on the SgNB , the SgNB and the UE shall delete the KSgNB-UPenc, K SgNB-UP-int, KSgNB-RRC-int and KSgNB-RRC-enc. The SgNB and UE shall also delete the S‑KgNB, if it was not deleted earlier.

The UP integrity protection policy indicates whether UP integrity protection shall be activated or not for all DRBs belonging to that E-RAB. The MME provides the UP integrity protection policy for each E-RAB to the MeNB during the Attach/Dedicated bearer activation/Dedicated bearer modification procedure as specified in TS 23.401 [2]. The MME receives UP integrity protection policy from SMF+PGW-C via SGW.

If the MeNB receives UP integrity protection policy from other entities, the MeNB shall forward the UP integrity protection policy together with the UE capability indicating support of user plane integrity protection with SgNB in EN-DC.

Editor’s note: Its FFS how the UE indicates support of user plane integrity protection with SgNB in EN-DC, e.g. whether EIA7 bit in the UE EPS security capabilities is used or whether a new indication is defined in e.g. UE NR security capability.

## E.3.3 Activation of encryption/decryption/integrity protection of DRBs and encryption/decryption/integrity protection of SRB

The dual connectivity procedure with activation of encryption/decryption and integrity protection of Split and/or Non-Split SgNB terminated DRB(s) (i.e. a DRB for which PDCP is located in the SgNB) and/or activation of encryption/decryption and integrity protection of an SgNB terminated SRB (i.e. a SRB for which PDCP is located in the SgNB) follows the steps outlined on the Figure E.3.3-1.



Figure E.3.3-1. SgNB encryption/decryption and integrity protection activation

1. The UE and the MeNB establish the RRC connection.

2. Before the MeNB decides to use dual connectivity for some DRB(s) and/or an SRB with the SgNB, the MeNB shall check whether the UE has NR capability and is authorized to access NR. The MeNB sends SgNB Addition Request to the SgNB over the X2-C to negotiate the available resources, configuration, and algorithms at the SgNB. . The MeNB computes and delivers the S-KgNB to the SgNB if a new key is needed. The UE NR security capability shall also be sent to SgNB. If the UE supports UP integrity protection with EPS (including user plane integrity protection with a SgNB in EN-DC), the SgNB Addition Request message shall additionally include UP integrity protection policy (either the one received from other network entities or the locally configured one if no UP integrity protection policy is received from other network entities).

NOTE 1: Void.

NOTE 2: Void.

3. The SgNB allocates the necessary resources and chooses the ciphering algorithm and integrity algorithms for the DRB(s) and SRB , if an SRB is to be established, which has the highest priority from its configured list and is also present in the UE NR security capability. If a new S-KgNB was delivered to the SgNB, then the SgNB calculates KSgNB-UP-int (if needed) and KSgNB-UP-enc as well as KSgNB-RRC-int and KSgNB-RRC-enc if an SRB is to be established. If the UE security capabilities indicates that the UE supports user plane integrity protection with a SgNB in EN-DC, then the SgNB shall use the UP IP policy received from the MeNB to determine whether to activate UP integrity protection. The SgNB shall activate UP integrity protection per DRB according to the UP integrity protection policy if it is received and shall indicate that to the UE.

4. The SgNB sends SgNB Addition Request Acknowledge to the MeNB indicating availability of requested resources and the identifiers for the selected algorithm(s) to serve the requested DRBs and/or SRB for the UE.

5. The MeNB sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SgNB. The MeNB shall include the SCG Counter parameter to indicate that the UE shall compute the S-KgNB for the SgNB if a new key is needed. The MeNB forwards the UE configuration parameters (which contains the algorithm identifier(s) and UP integrity indication received from the SgNB in step 4) to the UE (see section E.3.4.3 for further details).

NOTE 3: Since the message is sent over the RRC connection between the MeNB and the UE, it is integrity protected using the KRRCint of the MeNB. Hence the SCG Counter cannot be tampered with, and the UE can assume that it is fresh.

6. The UE accepts the RRC Connection Reconfiguration Command. The UE shall compute the S-KgNB for the SgNB if an SCG Counter parameter was included. The UE shall also compute KSgNB-UP-enc and and KSgNB-UP-int (if needed) as well as KSgNB-RRC-int and KSgNB-RRC-enc for the associated assigned DRBs and/or SRB. The UE sends the RRC Reconfiguration Complete to the MeNB. The UE activates the chosen encryption/decryption and integrity protection at this point.

7. MeNB sends SgNB Reconfiguration Complete to the SgNB over the X2-C to inform the SgNB of the configuration result. On receipt of this message, SgNB may activate the chosen encryption/decryption and integrity protection with UE. If SgNB does not activate encryption/decryption and integrity protection with the UE at this stage, SgNB shall activate encryption/decryption and integrity protection upon receiving the Random Access request from the UE.

## E.3.4 Derivation of keys for RBs with PDCP in the SgNB

### E.3.4.1 SCG Counter maintenance

The same SCG Counter is used for both SeNB and SgNB and the handling for SgNBs follow the procedures for SeNB given in E.2.4.1.

### E.3.4.2 Security key derivation

The UE and MeNB shall derive the security key S-KgNB of the target SgNB as defined in Annex A.15 of the present specification. KSgNB-UP-enc, KSgNB-UP-int, KSgNB-RRC-int and KSgNB-RRC-enc are derived from the S-KgNB both at the SgNB side and the UE side as shown on Figure E.3.4.2-1 using the function given in Annex A.19.



Figure E.3.4.2-1 Addition to the Key Hierarchy for the SgNB

### E.3.4.3 Negotiation of security algorithms

The UE NR security capabilities shall be indicated to the network using a new IE so that the support of EPS and NR algorithms can evolve independently. The UE shall send the UE NR security capabilities to the MME in Attach Request and (when possibly changing MME) TAU Request. To enable the usage of NR EN-DC with an MME that does not understand the UE NR security capabilities in the new IE, such an MME will drop the UE NR security capabilities and never save them in its UE context. An eNB that does not receive the UE NR security capabilities shall use the E-UTRAN security capabilities algorithms to create the supported UE NR security capabilities (see Annex E.10.3.2 for more details).

An MME that has the UE NR security capabilities shall send the UE NR security capabilities to the eNB in the S1-Initial Context Set-up message.

At S1-handover if the target MME receives the UE NR security capabilities from the source MME, the target MME shall send the UE NR security capabilities to the target eNB in the S1-AP Handover Request

At X2 handover, if the source eNB has the UE NR security capabilities, the source eNB shall send the UE NR security capabilities to the target eNB. These UE NR security capabilities should be the same as received from the MME on the S1 interface.

After a handover, it is possible that an eNB may have not received the UE NR security capabilities as the UE may have just been handed over from an eNB or MME that does not support the UE NR security capabilities. To overcome such a possible problem, the eNB shall create the UE NR security capabilities from the supported E-UTRAN security algorithms. To do this, the eNB shall use the mapping between the E-UTRAN security algorithms and NR security algorithms as per Annex E.3.10.2. When adding SgNB while establishing an EN-DC connection, the MeNB shall send these created UE NR security capabilities to the SgNB. Other than for adding an SgNB, the created UE NR security capabilities shall not be sent from the MeNB.

A target eNB that has received the UE NR security capabilities during handover shall include the UE NR security capabilities in the S1-PATH SWITCH-REQUEST message.

If an MME does not receive the UE NR security capabilities in the S1-PATH-SWITCH-REQUEST message from the target eNB to which the UE is connected to, or if an MME becomes aware that the eNB doesn’t know the UE NR security capabilities after an S1-handover, the MME should send the UE NR security capabilities to the target eNB via the PATH SWITCH REQUEST ACKNOWLEDGE message as specified in TS 36.413 [42], and the the target eNB shall store the UE NR security capabilities in the UE context.

When establishing one or more DRBs and/or a SRB for a UE at the SgNB, as shown on Figure E.3.3-1, the MeNB shall send the UE NR security capabilities associated with the UE in the SgNB Addition/Modification procedure. Upon receipt of this message, the SgNB shall identify the needed algorithm(s) with highest priority in the locally configured priority list of algorithms that is also present in the received UE NR security capabilities and include an indicator for the locally identified algorithm(s) in SgNB Addition/Modification Request Acknowledge.

The MeNB shall forward the indication to the UE during the RRCConnectionReconfiguration procedure that establishes the SgNB terminated DRBs and/or SgNB terminated SRB in the UE. The UE shall use the indicated encryption algorithms for the SgNB terminated DRBs and/or SgNB terminated SRB and the indicated integrity algorithm for the SgNB terminated SRB and/or SgNB terminated DRBs.

NOTE: Void.

## E.3.5 S-KgNB update

### E.3.5.1 S-KgNB update triggers

The system supports update of the S-KgNB. The MeNB may update the S-KgNB for any reason by using the S-KgNB update procedure defined in clause E.3.5.2 of the current specification. The SgNB shall request the MeNB to update the S-KgNB over the X2-C, when uplink or downlink PDCP COUNTs are about to wrap around for any of the SgNB terminated DRBs or SgNB terminated SRB.

If the MeNB re-keys its currently active KeNB in an AS security context the MeNB shall update any S-KgNB associated with that AS security context. This retains the two-hop security property for X2-handovers.

### E.3.5.2 S-KgNB update procedure

If the MeNB receives a request for S-KgNB update from the SgNB or decides on its own to perform S-KgNB update (see clause E.3.5.1), the MeNB shall compute a fresh S-KgNB and increment the SCG Counter, as defined in clause E.2.4. Thenthe MeNB shall performa SgNB Modification procedure to deliver the fresh S-KgNB to the SgNB. The MeNB shall provide the value of the SCG Counter used in the derivation of the S-KgNB to the UE in an integrity protected RRC procedure. The UE shall derive the S-KgNB as described in clause E.2.4.

Whenever the UE or SgNB start using a fresh S-KgNB, they shall re-calculate KSgNB-UP-int, KSgNB-UP-enc, KSgNB-RRC-int and KSgNB-RRC-enc from the fresh S-KgNB.

## E.3.6 Handover procedures

During S1 and X2 handover, the DRB connection between the UE and the SgNB shall be released, and the AS SC security context at SgNB and UE shall be deleted since it shall not be used again.

## E.3.7 Periodic local authentication procedure

SgNB may request the MeNB to execute a counter check procedure specified in clause 7.5 of this specification to verify the value of the PDCP COUNT(s) associated with DRB(s) offloaded to the SgNB. To accomplish this, the SgNB shall communicate this request, including the expected values of PDCP COUNT(s) and associated radio bearer identities (which are identified by E-RAB Id(s) in X2AP), to the MeNB over the X2-C.

If the MeNB receives a RRC counter check response from the UE that contains one or several PDCP COUNT values (possibly associated with both MeNB and SgNB), the MeNB may release the connection or report the difference of the PDCP COUNT values to the serving MME or O&M server for further traffic analysis for e.g. detecting the attacker.

## E.3.8 Radio link failure recovery

Since the MeNB holds the control plane functions even in dual connectivity, the UE runs the RRC re-establishment procedure with the MeNB as specified in clause 7.4.3 of the present specification.

NOTE: During the RRC re-establishment procedure, the DRB(s) offloaded between the UE and the SgNB is (are) released. If MeNB still want to offload DRB(s) to SgNB, SgNB addition is performed as specified in E.3.2.

## E.3.9 Avoiding key stream reuse caused by DRB type change

When a DRB changes from a MeNB terminated DRB (i.e. a DRB for which PDCP is located in the MeNB) to a SgNB terminated DRB and then changes back to a MeNB terminated DRB, then key stream reuse is possible. MeNB shall implement a mechanism to prevent key stream reuse.

## E.3.10 Protection of the traffic between the UE and SgNB

### E.3.10.1 General

The ciphering protection shall be applied between the UE and gNB at the PDCP layer. The integrity protection shall be applied to the SRB and DRB between the UE and gNB at the PDCP layer.

The inputs to the integrity and ciphering algorithms are the same as the input for the algorithms in LTE. Both the UE and SgNB shall support the following algorithms described in Annex D of TS 33.501 [43].

NEA0 (which is the same as EEA0) for both RRC and UP confidentiality.

128- NEA1 (which is the same as 128-EEA1) for both RRC and UP confidentiality.

128-NEA2 (which is the same as 128-EEA2) for both RRC and UP confidentiality.

128-NIA1 (which is the same as 128-EIA1) for both RRC and UP integrity protection.

128-NIA2 (which is the same as 128-EIA2) for both RRC and UP integrity protection.

Both the UE and SgNB may support the following algorithms described in Annex D of TS 33.501 [43].

128-NEA3 (which is the same as 128-EEA3) for both RRC and UP confidentiality.

128-NIA3 (which is the same as 128-EIA3) for both RRC and UP integrity protection .

The UE and SgNB shall not use NIA0 (which is the same as EIA0) between the UE and SgNB.

NOTE 1: Void.

NOTE 2: Void.

### E.3.10.2 Creating the mapped UE NR security capabilities

The MeNB that does not have the UE NR security capabilities shall create them as follow:

- Set the support of NEA0, 128-NEA1, 128-NEA2, 128-NEA3, 128-NIA1, 128-NIA2, 128-NIA3 to the same as EEA0, 128-EEA1, 128-EEA2, 128-EEA3, 128-EIA1, 128-EIA2, 128-EIA3 respectively; and

- Set the rest of the bits to 0.

Editor’s note: Its FFS how the UE indicates support of user plane integrity protection with SgNB in EN-DC, e.g. whether EIA7 bit in the UE EPS security capabilities is used or whether a new indication is defined in e.g. UE NR security capability, and what the implications are when creating the mapped UE NR security capabilities.

This mapping of E-UTRAN security algorithms support to NR security algorithms support means that for the purposes of dual connectivity to SgNB, the UE shall have the same support for 128-NEA1 as 128-EEA1, 128-NEA2 as 128-EEA2, 128-NEA3 as 128-EEA3, 128-NIA1 as 128-EIA1, 128-NIA2 as 128-EIA2 and 128-NIA3 as 128-EIA3.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*