**3GPP TSG-SA3 Meeting #104-e *DRAFT r1 S3-213266***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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:*** | Living CR for UPIP for LTE | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Vodafone | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPIP\_SEC\_LTE | | | | |  | ***Date:*** | | | 2021-08-07 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | This is living CR for UPIP, nothing is changed based on S3-212308. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This is living CR for UPIP. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification is not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.3.X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2 EPS key hierarchy

Requirements on EPC and E-UTRAN related to keys:

a) The EPC and E-UTRAN shall allow for use of encryption and integrity protection algorithms for AS and NAS protection having keys of length 128 bits and for future use the network interfaces shall be prepared to support 256 bit keys.

b) The keys used for UP, NAS and AS protection shall be dependent on the algorithm with which they are used.



Figure 6.2-1: Key hierarchy in E-UTRAN

The key hierarchy (see Figure 6.2-1) includes following keys: **KeNB, KNASint, KNASenc, KUPenc, KRRCint**,**KRRCenc** and **KUPint**

**- KeNB**is a key derived by ME and MME from KASME or by ME and target eNB.

Keys for NAS traffic:

**- 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 ME and MME from KASME, as well as an identifier for the integrity algorithm using the KDF as specified in clause A.7.

**- 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 ME and MME from KASME, as well as an identifier for the encryption algorithm using the KDF as specified in clause A.7.

Keys for UP traffic:

**- 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 ME and eNB from KeNB, as well as an identifier for the encryption algorithm using the KDF as specified in clause A.7.

**-** **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 RN and DeNB and between ME and eNB, from KeNB, as well as an identifier for the integrity algorithm using the KDF as specified in clause A.7.

Keys for RRC traffic:

**- KRRCint** is a key, which shall only be used for the protection of RRC traffic with a particular integrity algorithm.KRRCint is derived by ME and eNB from KeNB, as well as an identifier for the integrity algorithm using the KDF as specified in clause A.7.

**- KRRCenc** is a key, which shall only be used for the protection of RRC traffic with a particular encryption algorithm.KRRCenc is derived by ME and eNB from KeNB as well as an identifier for the encryption algorithm using the KDF as specified in clause A.7.

Intermediate keys:

**- NH** is a key derived by ME and MME to provide forward security as described in clause 7.2.8.

**- KeNB\*** is a key derived by ME and eNB when performing an horizontal or vertical key derivation as specified in clause 7.2.8 using a KDF as specified in clause A5.

Figure 6.2-2 shows the dependencies between the different keys, and how they are derived from the network nodes point of view. Figure 6.2-3 shows the corresponding relations and derivations as performed in the ME. Two dashed inputs to a KDF means one of the inputs is used depending on the circumstances of the key derivation.

NOTE: Figures 6.2-2 and 6.2-3 do not cover the derivations at IRAT mobility (see clauses 9 and 10).

MME

HSS

CK,IK

256

256

KDF

256

256

SN id, SQN ⊕ AK

KeNB

KASME

256

SNCK,IK

ME

SN id, SQN ⊕ AK

KDF

256

KDF

KDF

KDF

256

KDF

KSN id, SQN ⊕ AK

eNB

KeNB

KNASenc

KeNB

KNASint

KASME

MME

256

ME

KNASenc

KNASint

2KDF

CK,IK

HSS

Trunc

256

Trunc

256

KDF

KDF

256

256

128

KN256

Trunc

Trunc

KRRCint

128

256

256

UP-enc-alg,

Alg-ID

256

KUPenc

KUPenc

256

256

NAS-enc-alg,

Alg-ID

NAS-int-alg,

Alg-ID

Physical cell ID, EARFCN-DL

NAS UPLINK COUNT

KeNB\*

256

256

nc

KDF

KDF

KDF

256

KUPenc

256

KUPenc

KUPenc

KRRCint

12128

256

Trunc

256

KUPenc

256

NH

KDF

KRRCint

Trunc

Trunc

KDF

KUPenc

256

Trunc

256

256

128

128

256

128

256

UP-enc-alg, Alg-ID

KDF

RRC-int-alg, Alg-ID

NH

RRC-enc-alg, Alg-ID

256

256

Physical cell ID, EARFCN-DL

256

KeNB

eNB

eNB

KeNB\*

KDF

KRRCenc

KRRCenc

256

256

128

Trunc

KDF

NH

SN id, SQN ⊕ AK

SN id, SQN ⊕ AK

NH

KeNB

256

KeNB

KeNB

256

KDF

Trunc

KASME

KASME

UP-int-alg, Alg-ID

KUPint

256

256

256

256

MME

MME

KUPint

128

SN id, SQN ⊕ AK

Figure 6.2-2: Key distribution and key derivation scheme for EPS (in particular E-UTRAN) for network nodes.

ME

CK,IK

KDF

256

256

SN id, SQN Å AK

KeNB

KASME

256

KDF

KDF

KDF

KDF

KNASenc

KNASint

KNASenc

KNASint

Trunc

Trunc

256

256

128

128

256

256

256

NAS-enc-alg,

Alg-ID

NAS-int-alg,

Alg-ID

NAS UPLINK COUNT

KDF

KDF

KUPenc

KRRCint

KUPenc

KRRCint

Trunc

Trunc

256

256

128

128

256

UP-enc-alg, Alg-ID

RRC-int-alg, Alg-ID

RRC-enc-alg, Alg-ID

256

256

Physical cell ID, EARFCN-DL

256

KeNB\*

KDF

KRRCenc

KRRCenc

256

256

128

Trunc

KDF

NH

NH

KeNB

256

256

KDF

Trunc

KUPint

256

256

KUPint

128

UP-int-alg, Alg-ID

Figure 6.2-3: Key derivation scheme for EPS (in particular E-UTRAN) for the ME.

As the figures 6.2-2 and 6.2-3 show, the length of KASME, KeNB and NH is 256 bits, 256-bit NAS, UP and RRC keys are always derived from KASME and KeNB respectively. In case the encryption or integrity algorithm used to protect NAS, UP or RRC requires a 128-bit key as input, the key is truncated and the 128 least significant bits are used. Figures 6.2-2 and 6.2-3 illustrate the truncation to 128 bits keys.

The function Trunc takes as input a 256-bit string, and returns a truncated output as defined in Annex A.7.

### \*\*\*\*\* NEXT CHANGE \*\*\*\*\*

### 7.3.2 UP integrity mechanisms

This subclause applies only to the user plane on the Un interface between RN and DeNB and Uu interface between UE and eNB:

The user plane data is integrity-protected by the PDCP protocol between the UE and the eNB and between the RN and the DeNB as specified in TS 36.323 [12]. Replay protection shall be activated when integrity protection is activated. Replay protection shall ensure that the receiver only accepts each particular incoming PDCP COUNT value once using the same AS security context.

The use and mode of operation of the 128-EIA algorithms are specified in Annex B.

The input parameters to the 128-bit EIA algorithms as described in Annex B are a 128-bit integrity key KUPint as KEY, a 5-bit bearer identity BEARER which value is assigned as specified by TS 36.323 [12], the 1-bit direction of transmission DIRECTION, and a bearer specific, time and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

The supervision of failed UP integrity checks shall be performed in the UE and the eNB, and in the RN and the DeNB. In case of failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the UE side or on the eNB side. This can also happen on the DeNB side or on the RN side.

NOTE: The handling of UP integrity check failures by an UE or by an RN is an implementation issue. TS 36.323 [12] intentionally does not mandate any action for a failed integrity check (not even sending an indication of failure to higher layers). Consequently, depending on the implementation, the message failing integrity check is, or is not, silently discarded. This is in contrast to the handling of a failed RRC integrity check by a UE, cf. the NOTE in clause 7.4.1 of the present document.

UE and the eNB shall derive UP integrity key as specified in Annex A.7.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

7.3.X UP integrity protection policy

If the UE indicates that it supports user plane integrity protection with EPC in EIA7 in the EPS security capability, the MME shall provide UP integrity protection policy for each E-RAB to the eNB 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.

Editor’s Note: How to address the issue that some existing MMEs may not copy all EEA/EIA bits from NAS signalling into S1AP or some existing eNB may not copy all the EEA/EIA bits from S1-AP signalling into X2AP signalling raised by RAN3 LS S3-212436 are ffs.

NOTE 1: The SMF+PGW-C can be locally configured with UP integrity protection and confidentiality policy. However, the SMF+PGW-C only sends UP integrity protection policy to the upgraded SGW. The SMF+PGW-C, SGW and MME can use GTP-C signalling compatibility concepts to jugde whether to send UP integrity protection policy to the peer.

The UP integrity protection policy shall indicate whether UP integrity protection shall be activated or not for all DRBs belonging to that E-RAB.

The eNB shall be locally configured with UP integrity protection policy. If the eNB receives UP integrity protection policy from the MME, the eNB shall use the received UP integrity protection policy, otherwise, the eNB shall use the locally configured UP integrity protection policy if EIA7 in the EPS security capability indicates that the UE supports user plane integrity protection with EPC.

NOTE 2: It is recommended that the locally configured UP integrity protection policy on eNB is set as “preferred”.

The eNB shall activate UP integrity protection per each DRB, according to the UP integrity protection policy, using RRC signalling as defined in clause 7.3.Y. If the UP integrity protection policy indicates "Required", the eNB shall activate UP integrity protection. If the eNB cannot activate UP integrity protection, and when the UP integrity protection policy is "Required", the eNB shall reject establishment of UP resources for the E-RAB and indicate reject-cause to the MME. If the UP integrity protection policy is " Not needed ", the eNB shall not activate UP integrity protection.

At an X2-handover from the source eNB to the target eNB, the source eNB shall include in the HANDOVER REQUEST message, the UP integrity protection policy and the corresponding E-RAB ID, if the UP integrity protection policy is received from other entities. If the target eNB does not receive the UP integrity protection policy, but the EIA7 in the EPS security capability indicates that the UE supports user plane integrity protection with EPC, the target eNB shall use its locally configured UP integrity protection policy to activate or deactivate the UP integrity protection for all DRBs belonging to the E-RAB.

If the received UP integrity protection policy is ‘Required’, the target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the MME. For the accepted E-RABs, the target eNB shall activate UP integrity protection per DRB according to the UP integrity protection policy and shall indicate that to the UE in the HANDOVER COMMAND by the source eNB.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection for an E-RAB is enabled at the target eNB, the UE shall generate or update the UP integrity protection key and shall activate UP integrity protection for the respective E-RAB.

NOTE 3: If the UP integrity protection policy is ‘Preferred’, it is possible to have a change in activation or deactivation of UP integrity after the handover.

Further, in the Path-Switch message, the target eNB shall send the UE's UP integrity protection policy and corresponding E-RAB ID to the MME. The sent UP integrity protection policy can either be the one received from source eNB or the locally configured one if the target eNB does not receive it from the source eNB, but the EIA7 in the EPS security capability indicates that the UE supports user plane integrity protection with EPC. If the MME receives UP integrity protection policy, the MME shall verify that the UP integrity protection policy received from the target eNB is the same as the UP integrity protection policy that the MME has locally stored. If there is a mismatch, the MME shall send its locally stored UE's UP integrity protection policy of the corresponding E-RABs to the target eNB. This UP integrity protection policy, if included by the MME, is delivered to the target eNB in the Path-Switch Acknowledge message. The MME may support logging capabilities for this event and may take additional measures, such as raising an alarm.

NOTE 4: An upgraded target eNB may not receive UE’s UP integrity protection policy from a legacy source eNB, thus, mismatch of UP integrity protection policy may not be regarded as an abnormal case. The upgraded target eNB can get UE’s UP integrity protection policy from the MME.

If the target eNB receives UE's UP integrity protection policy from the MME in the Path-Switch Acknowledge message, the target eNB shall update the UE's UP integrity protection policy with the received UE's UP integrity protection policy. If UE's current UP integrity protection activation is different from the determination of received UE's UP integrity protection policy, then the target eNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure to reconfigure the DRBs to activate or de-activate the UP integrity as per the received policy from MME.

At an S1-handover, the source MME shall send the UE's UP integrity protection policy to the target eNB via the target MME. Besides, the source eNB shall also send the UE’s UP integrity protection policy if received from the source MME to the target eNB in a source-to-target container. The target eNB shall use the UP integrity protection policy received from the MME and ignore the UP integrity protection received in the source-to-target container, if the target eNB does not receive the UP integrity protection policy from the MME, the target eNB shall use UP integrity protection policy received from the source eNB, if both is absent, but EIA7 in the EPS security capability indicates that the UE supports use of user plane protection with EPC, the eNB shall use locally configured UP integrity protection policy. The target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the source MME via the target MME. For all other E-RABs, the target eNB shall activate UP integrity protection per DRB according to the used UP integrity protection policy.

At interworking-handover from 5GS to EPS, the SMF+PGW-C provides the UE's UP integrity protection policy to the target eNB via the target MME. The target eNB shall determine from the UP integrity protection policy received from the SMF+PGW-C via the MME together with indication that the UE supports use of user plane protection with EPC whether to activate user plane integrity protection with the UE or not. If the target eNB does not receive the UP integrity protection policy from the SMF+PGW-C via the MME, but the UE indicates support of UP integrity protection with EPS , the eNB shall use locally configured UP integrity protection policy. The target eNB shall reject all E-RABs for which it cannot comply with the corresponding UP integrity protection policy and indicate the reject-cause to the source AMF via the target MME. For all other E-RABs, the target eNB shall activate UP integrity protection per DRB according to the used UP integrity protection policy.

Editor’s Note: Policy handling when dealing with legacy nodes (eNB/MME) during interworking is FFS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.3.X UP integrity protection activation mechanism

AS UP integrity protection activation shall be done as part of the DRB addition procedure using RRC Connection Reconfiguration procedure as described in this clause, see Figure 7.3.X -1.

As defined in Clause 7.3.Y, the MME may send the UP integrity protection policy to the eNB. If the MME does not send the UP integrity protection policy, the eNB may use locally configured UP integrity protection policy.



Figure 7.3.X-1: User plane (UP) integrity protection activation mechanism

1a. This RRC Connection Reconfiguration procedure which is used to add DRBs shall be performed only after RRC security and UP ciphering have been activated as part of the AS security mode command procedure defined in Clause 7.2.4.5 and the UE indicates that it supports use of user plane integrity protection with EPC.

1b. The eNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation containing indication for the activation of UP integrity protection for each DRB according to the security policy.

1c. If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the eNB does not have KUPint, the eNB shall generate KUPint and UP integrity protection for such DRBs shall start at the eNB.

2a. UE shall verify the RRC Connection Reconfiguration message. If successful, if UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have KUPint, the UE shall generate KUPint and UP integrity protection for such DRBs shall start at the UE.

2b. If the UE successfully verifies integrity of the RRC Connection Reconfiguration message, the UE shall send the RRC Connection Reconfiguration Complete message to the eNB.

If UP integrity protection is not activated for DRBs, the eNB and the UE shall not integrity protect the traffic of such DRB and shall not put MAC-I into PDCP packet.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# A.7 Algorithm key derivation functions

When deriving keys for NAS integrity and NAS encryption algorithms from KASME and algorithm types and algorithm IDs, and keys for RRC integrity, UP integrity, and RRC/UP encryption algorithms from KeNB, in the UE, MME and eNB the following parameters shall be used to form the string S.

- FC = 0x15

- P0 = algorithm type distinguisher

- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)

- P1 = algorithm identity

- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm type distinguisher shall be NAS-enc-alg for NAS encryption algorithms and NAS-int-alg for NAS integrity protection algorithms. The algorithm type distinguisher shall be RRC-enc-alg for RRC encryption algorithms, RRC-int-alg for RRC integrity protection algorithms, UP-enc-alg for UP encryption algorithms and UP-int-alg for UP integrity protection algorithms (see table A.7-1). The values 0x07 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

Table A.7-1: Algorithm type distinguishers

|  |  |
| --- | --- |
| Algorithm distinguisher | Value |
| NAS-enc-alg | 0x01 |
| NAS-int-alg | 0x02 |
| RRC-enc-alg | 0x03 |
| RRC-int-alg | 0x04 |
| UP-enc-alg | 0x05 |
| UP-int-alg | 0x06 |

The algorithm identity (as specified in clause 5) shall be put in the four least significant bits of the octet. The two least significant bits of the four most significant bits are reserved for future use, and the two most significant bits of the most significant nibble are reserved for private use. The entire four most significant bits shall be set to all zeros.

For NAS algorithm key derivations, the input key shall be the 256-bit KASME, and for UP and RRC algorithm key derivations, the input key shall be the 256-bit KeNB.

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 5th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annex E (normative): Dual connectivity

# E.1 Introduction

## E.1.1 General

This clause describes the security functions necessary to support a UE that is simultaneously connected to more than one eNB for the architectures for dual connectivity as described in TS 36.300 [30]. The security functions are described in the context of the functions controlling the dual connectivity.

## E.1.2 Dual Connectivity architecture with an SeNB

For dual connectivity architecture, which hosts PDCP in MeNB the security functions described for the single connectivity mode in this specification are sufficient. The reason for that they are sufficient, is that the end-point for the encryption and integrity protection remains in the MeNB. That is, from a security point of view, the PDCP packets are still processed in the same locations in the architecture; they have only travelled a different path via the SeNB.

The remainder of the present subclause deals with dual connectivity between an MeNB and an SeNB with the architecture as shown in Figure E.1. 2-1.



Figure E.1.2-1: Dual Connectivity architecture with an SeNB

When the MeNB establishes security between an SeNB 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-KeNB for the SeNB and sends it to the SeNB over the X2-C. To generate the S-KeNB, the MeNB associates a counter, called an SCG Counter, with the current AS security context. The SCG Counter is used as freshness input into S-KeNB derivations as described in the clause E.2.4, and guarantees, together with the other provisions in the present clause E, that the KUPenc and the KUPint derived from the same S-KeNB is not re-used with the same input parameters as defined in Annex B of the present specification. The latter would result in key-stream re-use. The MeNB sends the value of the SCG Counter to the UE over the RRC signalling path when it is required to generate a new S-KeNB.

The communication established between the SeNB and the UE is protected at the PDCP layer using the AS Secondary Cell security context, or AS SC security context for short. The AS SC security context includes parameters as the AS security context described in clause 7 of the present specification, the S-KeNB replaces the KeNB. The UE and the SeNB derives the KUPenc and the KUPint from the S-KeNB as described in clause A.7, cf. also E.2.4.2.

# E.2 Dual connectivity offload architecture between eNBs

## E.2.1 Protection of the X2 reference point

The control plane signalling between MeNB and SeNB, that includes the transfer of the S-KeNB from the MeNB to the SeNB, over the X2 reference point shall be confidentiality and integrity protected using X2-C security protection as described in clause 5.3.4a and clause 11 of the present specification. Any user plane data between MeNB and SeNB over X2 reference point shall be confidentiality and integrity protected using X2-U security protection as described in clause 5.3.4 and clause 12 of the present specification.

## E.2.2 Addition and modification of DRB in SeNB

When executing the SeNB Addition procedure (i.e. the initial offload of one or more radio bearers to the SeNB), or the SeNB Modification procedure requiring an update of S-KeNB, the MeNB shall derive an S- KeNB as defined in clause E.2.4, which results in a fresh S-KeNB. The MeNB shall forward the generated S-KeNB to the SeNB during the SeNB Addition procedure or SeNB Modification procedure requiring key update.

Note: Refer to TS 36.300 [30] for definition of the SeNB Addition and SeNB Modification procedures.

The SeNB shall derive a key KUPenc and KUPint from the received S-KeNB as defined in clause E.2.4 of the present specification and use it for all radio bearers that were being added.

At any point of time, the same KUPenc is used for encrypting all radio bearers between the SeNB and the UE and the same KUPint is used for integrity protection of all radio bearers between the SeNB and the UE. Once the KUPenc and the KUPint have been derived from the S-KeNB, the SeNB and UE may delete the S-KeNB.

The MeNB shall provide the value of the SCG Counter used in the derivation of the S-KeNB to the UE in the SeNB Addition procedure adding the radio bearer(s) in the UE. The UE shall derive the S-KeNB, KUPenc and KUPint as described in clause E.2.4.

When executing the procedure for adding subsequent radio bearer(s) to the same SeNB, the MeNB shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last S-KeNB change.

If the MeNB cannot allocate an unused radio bearer identity for a new radio bearer in the SeNB, due to radio bearer identity space exhaustion, the MeNB shall increment the SCG Counter and compute a fresh S-KeNB, and then shall perform a SeNB Modification procedure to update the S-KeNB. The MeNB may choose to update the S-KeNB instead of assigning a new radio bearer identity even when the latter would have been possible.

If the SeNB receives a new S-KeNB from the MeNB during the SeNB Modification procedure, the SeNB shall use the KUPenc and KUPint derived from the new S-KeNB as encryption key and integrity key for all the radio bearer (s).

If the UE receives a new SCG Counter in SeNB Addition/Modification procedure, then the UE shall use the KUPenc derived from the new S-KeNB, as the encryption key and integrity key for all the radio bearer(s) established with the SeNB.

When the last radio bearer on the SeNB is released, the SeNB Release procedure is performed; the SeNB and the UE shall delete the KUPenc and KUPint. The SeNB and UE shall also delete the S‑KeNB, if it was not deleted earlier.

## E.2.3 Activation of encryption/decryption

The DRB offload procedure with activation of encryption/decryption and integrity protection follows the steps outlined on the Figure E.2.3-1.



Figure E.2.3-1. SeNB encryption/decryption activation

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

2. The MeNB decides to offload the DRB(s) to the SeNB. The MeNB sends SeNB Addition Request to the SeNB over the X2-C to negotiate the available resources, configuration, and algorithms at the SeNB. The MeNB computes and delivers the S-KeNB to the SeNB as necessary. UE EPS security capability should also be sent to SeNB. If the UE supports UP integrity protection with EPS, the SeNB 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).

3. The SeNB allocates the necessary resources and chooses the ciphering algorithm which has the highest priority from its configured list and is also present in the UE EPS security capability. If the UE supports user plane integrity protection, then the SeNB shall use the UP IP policy received from the MeNB to determine whether to activate UP integrity protection. The SeNB 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.

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

4. The SeNB sends SeNB Addition Request Acknowledge to the MeNB indicating availability of requested resources and the identifiers for the selected ciphering algorithm and integrity algorithm to serve the requested DRB for the UE.

5. The MeNB sends the RRC Connection Reconfiguration Request to the UE instructing it to configure a new DRB for the SeNB. The MeNB shall include the SCG Counter parameter to indicate that the UE shall compute the S-KeNB for the SeNB, the KUPenc and the KUPint associated with the assigned bearer. The MeNB forwards the UE configuration parameters (which contains the algorithm identifier received from the SeNB in step 4) to the UE (see section E.2.4.3 for further details).

NOTE: 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 and shall compute the S-KeNB for the SeNB. The UE shall also compute the KUPenc and the KUPint for the associated assigned DRB on the SeNB. The UE sends the RRC Reconfiguration Complete to the MeNB. The UE activates encryption/decryption and integrity protection once S-KeNB and KUPenc are derived.

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

## E.2.4 Derivation of keys for the DRBs in the SeNB

### E.2.4.1 SCG Counter maintenance

The MeNB shall associate a 16-bit counter, SCG Counter, with the EPS AS security context.

The SCG Counter is used when computing the S-KeNB. The UE and the MeNB shall treat the SCG Counter as a fresh input to S-KeNB derivation. That is, the UE assumes that the MeNB provides a fresh SCG Counter each time and does not need to verify the freshness of the SCG Counter.

NOTE: An attacker cannot, over the air modify the SCG Counter and force re-use of the same SCG Counter. The reason for this is that the SCG Counter is delivered over the RRC connection between the MeNB and the UE, and this connection is both integrity protected and protected from replay.

The MeNB maintains the value of the counter SCG Counter for a duration of the current AS security context between UE and MeNB. The UE does not need to maintain the SCG Counter after it has computed the S-KeNB since the MeNB provides the UE with the current SCG Counter value when the UE needs to compute a new S-KeNB.

The MeNB that supports the DRB offload shall set the SCG Counter to ‘0’ when the KeNB in the associated AS security context is established. The MeNB shall set the SCG Counter to ‘1’ after the first calculated S- KeNB, and monotonically increment it for each additional calculated S- KeNB. The SCG Counter value '0' is hence used to calculate the first S-KeNB.

If the MeNB decides to turn off the offload connection and later decides to re-start the offloading to the same SeNB, the SCG Counter value shall keep increasing, thus keeping the computed S-KeNB fresh.

The MeNB shall refresh the KeNB of the AS security context associated with the SCG Counter before the SCG Counter wraps around. Re‑freshing the KeNB is done using intra cell handover as described in clause 7.2.9.3 of the present specification. When this KeNB is refreshed, the SCG Counter is reset to '0' as defined above.

### E.2.4.2 Security key derivation

The UE and MeNB shall derive the security key S-KeNB of the target SeNB as defined in Annex A.15 of the present specification.

The addition to the LTE key hierarchy with derivation of the S-KeNB is shown on Figure E.2.4.2-1.



Figure E.2.4.2-1 Addition to the Key Hierarchy for the SeNB

The SeNB and the UE shall further derive the ciphering key KUPenc for ciphering and the integrity key KUPint for integrity protection of the User Plane over the DRB. This derivation is performed according to Annex A.7 using the S-KeNB as the input key and the input string S formed using the IDs of the SeNB selected algorithm to the KDF.

NOTE: Void.

### E.2.4.3 Negotiation of security algorithms

When establishing one or more DRBs for a UE at the SeNB, as shown on Figure E.2.3-1, the MeNB shall forward the UE EPS security capabilities associated with the UE in the SeNB Addition/Modification procedure.

Upon receipt of this message, the SeNB shall identify the AS encryption algorithm with highest priority in the locally configured priority list of AS encryption algorithms that is also present in the received UE EPS security capabilities and include an indicator for the locally identified AS encryption algorithm in SeNB Addition/Modification Request Acknowledge.

Upon receipt of this message, if integrity protection is activated then the SeNB shall identify the AS integrity algorithm with highest priority in the locally configured priority list of AS integrity algorithms that is also present in the received UE EPS security capabilities and include an indicator for the locally identified AS integrity algorithm in SeNB Addition/Modification Request Acknowledge.

The MeNB shall forward the indication to the UE during the RRCConnectionReconfiguration procedure that establishes the SCG DRBs in the UE. The UE shall use the indicated encryption algorithm and integrity algorithm for the SCG DRBs.

NOTE 1: The UE uses one encryption algorithm for encryption of SRB and any potential DRB(s) established with MeNB, and a same or different encryption algorithm for encryption of DRB(s) established with SeNB.

NOTE 2: The UE uses one integrity algorithm for integrity of SRB and any potential DRB(s) established with MeNB, and a same or different integrity algorithm for integrity protection of DRB(s) established with SeNB.

## E.2.5 S-KeNB update

### E.2.5.1 S-KeNB update triggers

The system supports update of the S-KeNB. The MeNB may update the S-KeNB for any reason by using the S-KeNB update procedure defined in clause E.2. 5.2 of the current specification. The SeNB shall request the MeNB to update the S-KeNB over the X2-C, when uplink or downlink PDCP COUNTs are about to wrap around for any of the DRBs.

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

### E.2.5.2 S-KeNB update procedure

If the MeNB receives a request for S-KeNB update from the SeNB or decides on its own to perform S-KeNB update (see clause E.2.5.1), the MeNB shall compute a fresh S-KeNB and increment the SCG Counter, as defined in clause E.2.4. Thenthe MeNB shall performa SeNB Modification procedure to deliver the fresh S-KeNB to the SeNB. The MeNB shall provide the value of the SCG Counter used in the derivation of the S-KeNB to the UE in an integrity protected RRC procedure. The UE shall derive the S-KeNB and KUPenc as described in clause E.2.4.

Whenever the UE or SeNB start using a fresh S-KeNB, they shall re-calculate the KUPenc and the KUPint from the fresh S-KeNB.

## E.2.6 Handover procedures

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

## E.2.7 Periodic local authentication procedure

SeNB 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 SeNB. To accomplish this, the SeNB 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 SeNB), 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.2.8 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 SeNB is (are) released. If MeNB still want to offload DRB(s) to SeNB, SeNB addition is performed as specified in E.2.2.

## E.2.9 Avoiding key stream reuse caused by DRB type change

When a MCG DRB changes to SCG DRB and then changes back to MCG DRB, the key stream reuse is possible. MeNB shall implement a mechanism to prevent key stream reuse.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 5th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 6th 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 6th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 7th 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.

## 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).

Editor’s Note: Whether selection of SgNB will be enhanced is ffs.

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.

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 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 7th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*