**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212773-r1***

**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:*** | User Plane Integrity Protection Policy Handling in DC | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***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 in DC is not specified yet | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add text for UP IP policy handling in DC | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification is not complete. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex E | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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 (including user plane integrity protection with a SgNB in EN-DC), 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 EIA7 in the UE EPS security capabilities indicates that 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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*