**3GPP TSG RAN WG2#125bis R2-240XXXX**

**Changsha, China, 15th - 19th April 2024**

**Title: [Draft] LS on security handling for inter-CU LTM in non-DC cases**

**Response to:**

**Release:** **Rel-19**

**Work Item: NR\_Mob\_Ph4-Core**

**Source:** **[Draft] Apple ~~RAN WG2~~**

**To: SA WG3**

**Cc:** **RAN WG3**

**Contact person: Naveen Palle**

 **naveen (.) palle at apple (.) com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachment: None**

**1. Overall Description:**

Based on the following WID objective of R19 Mob enhancement, RAN2 discussed the aspect of inter-CU LTM with security key change and views the following options as possible directions (not mutually exclusive or comprehensive) for handling the key change as part of inter-CU LTM cell switch.As for reference, Rel-18 intra-CU LTM cell switch procedure at stage-2 level is specified in TS 38.300 clause 9.2.3.5.

|  |
| --- |
| * + Specify support for subsequent LTM mobility procedures aiming to avoid RRC configuration between cell switches as per Rel-18 LTM
		- Coordination with SA3 needed with respect to security key handling
 |

**Option 1:** Use a new information in MAC CE to deliver the security information. Whether the UE uses horizontal or vertical key derivation is derived from this new information in MAC CE (which is currently, neither integrity protected nor ciphered).

 **Option 1A:** NCC value to be used at inter-CU LTM execution is included in LTM cell switch command MAC CE.

 **Option 1B:** UE is preconfigured with a list of NCC values and association to the indices in a ciphered and integrity protected message (in RRC), and the index of an NCC is included in LTM cell switch command MAC CE.

**Option 2:** Similar to Rel-18 S-CPAC key update mechanism, the UE is preconfigured from the source gNB with a list of NCC values **per CU** using dedicated RRC signalling (that is both integrity protected and ciphered). It is expected that the participating gNBs (CUs) would need to be aware of the list and how the UE applies the list during handovers.

**Option 2A:** UE chooses the first unused NCC for the target CU upon an inter-CU LTM execution.

 **Option 2B:** As an alternative to choosing the next unused NCC (as in Option 2A), horizontal key derivation is used in this option if the LTM cell switch is between the same two CUs.

**Option 3:** After the execution of inter-CU LTM cell switch, the participating gNBs are expected to be updated with new K-gNB\* to be used for the next inter-CU LTM cell switch. The UE and CN are aware of how the UE would use the next NCC value.

 **Option 3A:** UE determines the following NCC to use by itself (e.g., increase by 1) after subsequent inter-CU LTM execution.

 **Option 3B:** UE is pre-configured by CN (via source gNB RRC signalling) with a list of NCC valuesand the UE chooses the first unused NCC as the next NCC value.

**Option 4:** After every inter-CU LTM cell switch execution, for vertical key derivation based security change, the UE is provided with the NCC to be used for the next inter-gNB CU LTM switch via dedicated RRC signaling. This implies that every inter-CU LTM switch which is vertically derived security key based, needs a prior RRC message to inform the UE which NCC to use for this inter-CU LTM switch.

RAN2 assumes that both horizontal and vertical derivation used in L3 handover could be supported for inter-CU LTM.

RAN WG2 agreed also to support mixture of subsequent inter-CU LTM and subsequent intra-CU LTM after an inter-CU or intra-CU LTM switch. Please note that the current number of candidate cells within intra CU case (release 18) is 8. This number might be increased (subject to further discussions in RAN WG2).

RAN WG 2 will consider Inter-CU with DC configured at a later stage. The above directions are intended for inter-CU LTM without DC case.

**2. Actions:**

**To SA3**

**ACTION:** RAN2 respectfully asks SA3 to take the above information related to security key change for Inter-CU LTM into account and comment on the below questions:

1. RAN2 asks SA3 to inform RAN2 if any of the above options are not acceptable from security perspective and clarify any modifications that could make the solutions acceptable (including the assessment on the impact from the needed signalling between participating network nodes).
2. RAN2 requests SA3 whether, for each option, the change of security algorithm or the change of key set indicator is to be supported for inter-CU LTM.

**3. Date of Next RAN WG2 Meetings:**

TSG RAN WG2 Meeting #126 20 - 24 May 2024  Fukuoka, Japan

TSG RAN WG2 Meeting #127 19 - 23 Aug 2024  Maastricht, Netherlands