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

**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:** **Apple [To be 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 key-change and views the following options as directions for handling the key change as part of inter-CU LTM cell switch:

|  |
| --- |
| * + 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 new information in MAC CE to deliver the security info. Whether the UE uses horizontal or vertical derivation is derived from this new information in MAC CE (neither integrity protected nor ciphered).

 **Option 1A:** NCC value to use is included as MAC CE parameter to be used at inter-CU LTM execution.

 **Option 1B:** UE is preconfigured with a NCC value list and association to the index in a secured way (in RRC), and the index of NCC is included as MAC CE parameter.

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

**Option 3:** The participating gNBs are expected to be updated with new K-gNB\* with the **next** to be used NCC after the execution of the **current** inter-CU LTM cell switch. 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 (eg., increase by 1) after subsequent inter-CU LTM execution.

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

**Option 4:** After every inter-CU LTM cell switch execution, for vertical derivation based security change, using RRC, the UE is provided with the NCC to be used for the next inter-gNB CU LTM switch. 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.

**Option 5:** If the subsequent cell switch is between the same gNB-CU pair (i.e., the new source switches the UE back to the old source cell), the option of using horizontal derivation more than once, as long as the UE remains in the same pair

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 extended (subject to feather discussions in RAN WG2).

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

RAN WG2 would like to highlight that one of the benefits of LTM mobility is considered to be reduced signalling overhead and therefore it would be of benefit if SA3 could take this aspects into account during security related evaluations.

**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 requests SA3 to inform RAN2 if any of the above options are not acceptable from security perspective (including the assessment on the impact from needed signalling between participating network nodes).
2. From SA3 perspective, among the acceptable options from option 2 and option 3, RAN2 requests if horizontal derivation is also needed/allowed for RAN2 to specify.
3. If Option 1 is acceptable, RAN2 requests SA3 whether, via MAC CE, the change of security algorithm or the change of key set indicator is to be supported in 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