**3GPP TSG-SA3 Meeting #116 *S3-242285***

Jeju, South Korea, 20th - 24th May 2024

**Source: Samsung**

**Title: Summary on the contributions submitted for security handling of inter-CU LTM in non-DC cases**

**Document for: Information**

**Agenda Item: 3**

# 1 Summary

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tdoc** | **Company** | **Option 1** | | **Option 2** | | **Option 3** | | | **Option 4** | **Company stand** |
|  |  | **Option A** | **Option B** | **Option A** | **Option B** | **Option A** | | **Option B** |  |  |
| [**S3-241897**](https://protect2.fireeye.com/v1/url?k=5aa64609-3b2d533f-5aa7cd46-74fe485fffe0-886fe62fad9e8c4d&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-241897.zip) | ZTE | Signalling between gNBs is needed to transfer the NCC.    Can be done in MAC CE if protected. | Additional signalling between gNB and core network required to configure the NCC list.  Can be done in MAC CE if protected. | Signalling between gNBs is required for NCC transmission. Complicated signalling to transfer the changed NCC list to the gNBs.  RRC message can carry security/algorithm key change indicator + NCC | | RRC reconfiguration message may be needed for re-synchronization | | Signalling between the source gNB and the UE is required | Legacy handover procedure (e.g. Xn handover) is likely to be reused but is contrary to the high efficiency of subsequent LTM (no new RRC reconfiguration) | Providing evaluation of each options.  No explictpreference as of now. |
| [**S3-241898**](https://protect2.fireeye.com/v1/url?k=17b926d9-763233ef-17b8ad96-74fe485fffe0-185def4bc4ab1e84&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-241898.zip) | ZTE |  | | | | | | | | Providing evaluation of each options.  No preference as of now. |
| [**S3-242044**](https://protect2.fireeye.com/v1/url?k=f41a314c-9591247a-f41bba03-74fe485fffe0-dcc3fc7125b718ab&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242044.zip) | Intel | Least secure as it does not provide integrity protection for the NCC value | | Minimizing signalling at the LTM cells switch as both UE and candidate cells are preconfigured and do not require a key update after every LTM cell switch, but it requires updates to CN to provide multiple {NH, NCC} pairs. | | Unclear and seems to depend on certain rules that reduce flexibility for the network. | | | most secure as it provides key separation but requires key update signaling to all the prepared gNBs after every LTM cell switch | Prefers option 2 or option 4 |
| [**S3-242055**](https://protect2.fireeye.com/v1/url?k=0aa98015-6b229523-0aa80b5a-74fe485fffe0-1ad79db152a8ee19&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242055.zip) | Intel |  | | | | | | | | Prefers option 2 or option 4, option 4 more secure |
| [**S3-242080**](https://protect2.fireeye.com/v1/url?k=32a74fa6-532c5a90-32a6c4e9-74fe485fffe0-83cc534e1a0e4ef2&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242080.zip) | vivo | Minimizes signaling. UE and candidate cells preconfigured and do not require a key update after every LTM cell switch, but it requires updates to CN to provide multiple {NH, NCC} pairs. | | unclear due to the absence of RAN or CN interaction procedures  further details needed on interaction | | unclear due to the absence of RAN or CN interaction procedures  further details needed on interaction | | | Secure option and follows current security procedure for Xn handover. | For Q1: Prefers option 1 and option 4  For Q2: Needs more time.  And ask for more details on option 2 and 3 |
| [**S3-242100**](https://protect2.fireeye.com/v1/url?k=08c30c1f-69481929-08c28750-74fe485fffe0-711a5bf49caa1df7&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242100.zip) | OPPO | Option 1 is not acceptable from security perspective, unless the NCC value included in the MAC CE is protected | | Some measures are needed to address the issue on NCC running-out. | | NH parameter needs to be distributed from the AMF to the target gNB. And the source gNB cannot access the NH parameter belonging to the target gNB. | | | NCC value is carried by RRC signalling as in the legacy L3 based handover. Contradicts the design objective. | Provide feedback to RAN2 |
| [**S3-242101**](https://protect2.fireeye.com/v1/url?k=e5cff6a3-8444e395-e5ce7dec-74fe485fffe0-6b0b09bc767a167e&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242101.zip) | OPPO |  | | | | | | | | Provide feedback in response and further study is needed in SA3 |
| [**S3-242105**](https://protect2.fireeye.com/v1/url?k=63438e2c-02c89b1a-63420563-74fe485fffe0-e4e59dd9e9dddf6f&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242105.zip) | Ericsson | Lack of cryptographic protection in MAC.  Does not prefer this as there may be sync issue with MSB of the NCC | | CU only has access to one NH value and one associated NCC value acting as an identifier for the NH value. It is unclear what other (NH, NCC) value pairs is intended to be included in the list is intended. | | UE determines the value on its own the risk for desynchronization increases. This is true for Option 3A, and possibly also for Option 3B if the CU has performed any action that may have cause the NCC to be increased between provisioning the UE with the value and the cell switch. | | | appears closest to how existing handover signalling. More details required to analyse. | Request further details from RAN2 to analyse the options.  No explicit preference as of now. |
| [**S3-242136**](https://protect2.fireeye.com/v1/url?k=32848a31-530f9f07-3285017e-74fe485fffe0-c60f35595ee8c192&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242136.zip) | Xiaomi | Prefer this as it aligns with existing key handling | Does not prefer because NCC value cannot be preconfigured by the gNB | Does not prefer because NCC value cannot be preconfigured by the gNB | | Does not prefer as UE needs to determine the NCC | Does not prefer because NCC value cannot be preconfigured by the gNB | | Prefer this as it aligns with existing key handling | But thinks both option 1 A and 4 are not complete.  Wants to have study |
| [**S3-241886**](https://protect2.fireeye.com/v1/url?k=25ccd2e4-4447c7d2-25cd59ab-74fe485fffe0-6411eb501acc936a&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-241886.zip) | Apple |  | | | | | | | | Wants to study in SA3 and then get back to RAN2 |
| [**S3-242306**](https://protect2.fireeye.com/v1/url?k=0117e896-609cfda0-011663d9-74fe485fffe0-ddc4c4282e86206a&q=1&e=448d7433-6766-4700-acc3-3fa63f7b94f4&u=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_116_Jeju%2FDocs%2FS3-242306.zip) | LG |  | | | | | | | | Wants to study in SA3 and then get back to RAN2 |

# 2 Annex

**Excrept from S3-241773/R2-2404037 on the options**

|  |
| --- |
| **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:** the NCC value to be used at inter-CU LTM execution is included in the LTM cell switch command MAC CE.  **Option 1B:** the UE is preconfigured with a list of NCC values in a ciphered and integrity protected RRC message and the index of an NCC value in the list is included in the 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 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 LTM cell switches:  **Option 2A:** UE chooses the first unused NCC for the target CU upon 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:** The UE determines the following NCC value to use by itself (e.g., increase by 1) after subsequent inter-CU LTM execution.  **Option 3B:** UE is pre-configured by the CN (via source gNB RRC signalling) with a list of NCC values and the UE chooses the first unused NCC value as the next NCC value.  **Option 4:** After every inter-CU LTM cell switch execution, the UE is provided via RRC signalling with the NCC value to be used by the UE for key derivation at the next inter-CU LTM cell switch. |