**3GPP TSG-SA3 Meeting #117 *S3-24ltm1***

Maastricht, Netherlands, 19th – 23rd August 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title:** **Discussion on Impact Analysis for Inter-CU LTM**

**Document for: Discussion**

**Agenda Item: 4.12**

# 1 Decision/action requested

***This document is for the presentation and discussion of the security impacts of the Inter-CU LTM options.***

# 2 References

*(Reference - in list form - should be made to previous related SA5/3GPP/etc. documents.)*

*(For changes against a draft TS/TR, a pseudo CR - a.k.a. pCR - will be provided using this Tdoc template. In this case, the number, name and version of the draft TS/TR used as base must be provided and the version must be the latest available version of the draft TS/TR.)*

[1] [S3-241773](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_116_Jeju/Docs/S3-241773.zip) (R2-2404037) LS on security handling for inter-CU LTM in non-DC cases

[2] TS 33.501, Security Architecture

[3] A. Peltonen at all “A Comprehensive Formal Analysis of 5G Handover”
[5G-handover-WISEC21.pdf (ethz.ch)](https://people.inf.ethz.ch/rsasse/pub/5G-handover-WISEC21.pdf)

[4] …

# 3 Rationale

## 3.1 Background and Motivation

For the WI on the inter-CU LTM with security key change, the RAN2 has discussed and collected options as possible directions for handling the key change as part of inter-CU LTM cell switch. The options have been documented and shared with SA3 by means of a LS [1]. Now, as part of the LS, the SA3 is requested to study the different options from security perspective and to give feedback if any of the listed options is not feasible or not acceptable from security perspective.

## 3.2 Methodology

The security analysis consists of three parts, as these are:

Part1: The functional behaviour and key-handling of 5G system at handover (see clause 6.9 of [2]) is taken as the basis. Specifically, the functional behaviour in case related parameters like NCC, NH, KgNB, and KNG-RAN\* which might become subject to attack vectors, mainly with the aim to alter or refuse any of these parameters. This Part1 analysis is related to 5G system in general and is therefore not directly related to LTM.

Part2: The functional specifics of each option will be elaborated. Their treatment of the related parameters like NCC, NH, KgNB, and KNG-RAN\* in the procedure.

Part3: The assessment will be separated in to two aspects, the security and functional related.

## 3.3 Key-Handling of 5G System at Handover

This clause is describing the Part1 of the analysis.

Below Figure 3.3-1 depicts the general principle of key handling for KNG-RAN\*/NH at handovers (refer to Figure 6.9.2.1.1-1 of [2]).



Figure 3.3-1: Model for the handover key chaining

**Observation#1: A horizontal and vertical key-derivation has been introduced.**

The difference between the horizontal and vertical key-derivation is that in the horizontal key-derivation the KNG-RAN\* will be generated from the current KgNB, while in the vertical key-derivation the KNG-RAN\* will be generated from the NH.

Below a security assessment on the horizontal and vertical key-derivation (refer to [3]):

“In horizontal key derivation (hkd), the current session key is used as the input key when deriving the next one. The downside of this method is that it does not provide forward security, since learning an old key enables the attacker to derive all subsequent keys. This can be avoided by using vertical key derivation (vkd), which unlike hkd does not use the previous key when deriving the next one. Instead, the new key is derived using an intermediate Next Hop (NH) parameter provided by the AMF. This means that forward security holds with respect to reveals of earlier session keys, as long as the long-term key KAMF remains secret.”

**Observation#2: The horizontal key-derivation doesn’t provide forward security compared to the vertical key-derivation.**

The NCC value is used as a ‘pointer’ to derive the NH value at the next handover, from this perspective any possible altering of the NCC value can be seen as sensitive.

Copied from TS 33.501 [2]:

“Whenever an initial AS security context needs to be established between UE and gNB/ng-eNB, AMF and the UE shall derive a KgNB and a Next Hop parameter (NH). The KgNB and the NH are derived from the KAMF. A NH Chaining Counter (NCC) is associated with each KgNB and NH parameter. Every KgNB is associated with the NCC corresponding to the NH value from which it was derived. At initial setup, the KgNB is derived directly from KAMF, and is then considered to be associated with a virtual NH parameter with NCC value equal to zero. At initial setup, the derived NH value is associated with the NCC value one.”

“If the current KgNB is to be changed, the gNB/ng-eNB and the UE shall derive a KNG-RAN\* as in Annex A.11/A.12 using target PCI, its frequency ARFCN-DL/EARFCN-DL, and either NH or the current KgNB depending on the following criteria: the gNB shall use the NH for deriving KNG-RAN\* if an unused {NH, NCC} pair is available in the gNB (this is referred to as a vertical key derivation), otherwise if no unused {NH, NCC} pair is available in the gNB, the gNB shall derive KNG-RAN\* from the current KgNB (this is referred to as a horizontal key derivation). The gNB shall send the NCC used for the KNG-RAN\*derivation to UE in HO Command message. The gNB/ng-eNB and the UE shall use the KNG-RAN\* as the KgNB, after handover.”

**Observation#3: At gNB side the existence of an unused {NH, NCC} pair is used to decide whether horizontal or vertical key derivation is to be used, and at the UE side the NCC counter is associated with each KgNB and NH parameter. The altering of the NCC value might lead into a key mismatch and generation failure or might lead into horizontal key derivation.**

## 3.4 Functional Description if the inter-CU LTM Options

### 3.4.1 Option 1



Figure 3.4.1-1: Framework Option 1

The following is applicable:

* In the preparation phase, the NCC value or the NCC index list will be transferred as part of RRC procedures (Step 5).
* In the LTM cell switch phase, either the NCC value or the NCC index will be sent as part of the MAC CE cell switch command (Step 9).

### 3.4.2 Option 2



Figure 3.4.2-1: Framework Option 2

The following is applicable:

* The source gNB is sending a handover request (Step 4) towards the target gNB and the target gNB is triggering the procedure for the generation and provision of a new {NH, NCC} pair (Step 5/6).
* The Source gNB is creating NCC list per CU and is sharing this with UE (Step 9).
* In the LTM cell switch phase, the UE chooses the first unused NCC from a list that corresponds to the target-CU (Step 16) and which refers to the Option 2A.
* For a handover between the “same CU’s”, then horizontal key-derivation will be applied (Step 18/19).

### 3.4.3 Option 3



Figure 3.4.3-1: Framework Option 3a

The following is applicable:

* In the LTM preparation phase, the target gNB will be provisioned with K\_NG\_RAN\* and NCC value (Step 5) and the UE will be provisioned with the next NCC value.
* In the LTM cell switch execution phase, the UE determines the next NCC value on its own.



Figure 3.4.3-1: Framework Option 3b

The following is applicable:

* In the LTM preparation phase, the target gNB upon handover request, will request a list of NCC values from the AMF (Step 6). The AMF is preparing the NCC lists and is sharing those in a response message (Step 8).
* In the LTM cell switch phase, the UE is selecting the next NCC value from the NCC list (Step 15).

### 3.4.3 Option 4



Figure 3.4.4-1: Framework Option 4

The following is applicable:

* The NCC value will be RRC signalled on demand.

## 3.5 Assessment Matrix

The outcome of the 5G system level analysis and the functional description of the Option 1 to 4 can be moved into an assessment matrix, as depicted by below Figure 3.5-1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Aspect for comparison** | **Option 1A** | **Option 1B** | **Option 2A** | **Option 2B** | **Option 3A** | **Option 3B** | **Option 4** |
| Use of horizontal key derivation | Yes | Yes | No | Yes | No | Yes | No |
| Lack of forward security due to HKD | Yes | Yes | No | Yes | No | Yes | No |
| Vulnerability from lack of MAC CE security | Yes | Yes | No | No | No | No | No |
| Pre-provision of key materials like KgNB | No | No | No | No | Yes | Yes | No |

Figure 3.5-1: Assessment Matrix

Observations:

* There is a separation in security related aspects and functional related aspects.
* The Option 1 is transferring the NCC related information as MAC CE. Three threat vectors can be taken into consideration, i.e.,
	1. the first one relates to eavesdrop the NCC value in the clear, in this case the attacker obtains knowledge about the next NCC value, this could be mitigated by encryption of the MAC CE, in this case the attacker still could start a brute-force-attack as the NCC size is 3bits.
	2. The second one relates to the unavailability of the NCC value at the target node (this refers to a Denial-of-Service attack), in this case the attacker is altering altering/flipping bits of MAC CE with the aim to alter the protected NCC values. On receive side if the integrity verification has failed, the received NCC value will be discarded, consequently a valid NCC value will be made unavailable, or the ciphertext has been altered such the after it’s decryption the cleartext (=NCC value) is not identical to the original NCC value. For all these altering/flipping the MAC CE (independent to whether these are protected or not) the attacker is driving to a DoS for the connection between a UE and the network, as in all cases the missing or wrong NCC is leading to a mismatch of the security context.
	3. The third one relates to spoofing/impersonation of the MAC CE, in this case the attacker might claim to be a valid source gNB. The spoofing/impersonation could be mitigated by peer authentication means.
* The Option 2A does not use horizontal key-derivation as a valid option, which is more positive, but then there are additional functional efforts to manage the NCC lists which can be seen as more negative.

The Option 2B has the horizontal key-derivation as an option, which is negative due to lack of forward security. The transfer the NCC list will be protected by AS security context.

* The Option 3A does not have horizontal key-derivation as a valid option, which is more positive. The UE will be provisioned with the next NCC value to be used.
* The Option 3B has the horizontal key-derivation as an option, which has the lack of forward security. The transfer of sensitive information will be protected by AS and NAS security context. The AMF is pre-provisioning the KgNB\*, therefore all target gNB will be equipped with key-material. This has the likelihood although that keys stays in the target gNBs for some time and some of them may not be used. This aspect of keys ‘hanging-around’ for some duration brings additional vulnerability of potential key leakage. Keys for the next two levels of handover that will be given to the target gNB, brings additional lack of forward security.
* The Option 4 is transferring all key derivation related information via secured RRC signalling, therefore there is no security vulnerability.

## 3.x Abbreviations

CU Central Unit

DoS Denail of Service

HKD Horizontal Key Derivation

LTM L1/L2 Triggered Mobility

MAC Medium Access Control

MAC CE MAC Control Element

NCC Next Counter Check

NH Next Hop

RRC Radio Resource Control

# 4 Detailed proposal

**Proposal: SA3 to take above into consideration for security analysis and inter-CU LTM concept decision.**