**3GPP TSG-SA3 Meeting #118 *draft\_S3-244324-r1***

**Hyderabad, India 14 – 18 October 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | ***draft*** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document on NR mobility enhancement | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung (Rapporteur) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NR\_Mob\_Ph4\_Sec | | | | |  | ***Date:*** | | | 2024-08-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | This draft CR is the living document based on the approved WID proposal on security aspects of NR mobility enhancement ([S3-242401](https://www.3gpp.org/ftp/Meetings_3GPP_SYNC/SA3/docs/S3-242401.zip)). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | This draft CR will capture the security procedures to support the inter-CU LTM in 5G systems based on RAN2 progress. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security aspects for inter-CU LTM in 5G system will not be supported | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Clause Annex α of this draft CR is only used to document the work on the different options considered for the security aspects of inter-CU LTM. This annex α will not be included when this draft CR is converted into CR. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | S3-243193, S3-243689 | | | | | | | | |

***Start of 1st Change***

#### 6.X.Y Security mechanism and procedures for inter-CU LTM

Editor’s Notes: This clause contains the security procedure for inter-CU LTM in 5G.

In the case where CU is acting as SN and MN is unchanged, the security mechanism and procedures for SCPAC as specified in clause 6.10.2.4 apply.

***End of 1st Change***

Annex α (Informative):   
Security mechanisms for Inter-CU LTM

Editor’s Notes: This clause contains the key issues and security solutions considered for analyzing the security mechanism and procedure for inter-CU LTM based on work progress in RAN WGs.

# 1 References

[1] 3GPP TS 38.300: "NR; NR and NG-RAN Overall description; Stage-2".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP LS S3‑241773: "LS on security handling for inter-CU LTM in non-DC cases (R2-2404037)".

[4] 3GPP TS 38.423: "Xn Application Protocol".

# 2 Key issues

Editor’s Note: This clause contains all the key issues identified for the WID NRmobenh\_sec\_Ph1.

## 2.1 Key Issue #1: Security aspects of inter-CU LTM Handover

### 2.1.1 Key issue details

Layer1/Layer 2 Triggered Mobility (LTM) is a procedure in which a gNB receives L1 measurement report(s) from a UE, and on their basis the gNB changes UE serving cell by a cell switch command signalled via a MAC CE. The cell switch command indicates an LTM candidate configuration that the gNB previously prepared and provided to the UE through RRC signalling. Then the UE switches to the target configuration according to the cell switch command.

Currently in Rel-18, LTM operation is only supported for mobility between cells within a gNB i.e., both intra-gNB-DU and intra-gNB-CU inter-gNB-DU (same CU) mobility [1]. In release-19, it is planned to enable it for between cells of different gNBs (inter-CU).

### 2.1.2 Security threats

Not Applicable

### 2.1.3 Potential security requirements

The 5GS shall support key handling for inter-CU LTM based cell switch scenario.

The 5GS shall support security mechanism for the scenarios/features decided and specified by the RAN WGs for inter-CU LTM based cell switch scenario.

NOTE: There should be no impact to existing Layer 3 mobility.

## 2.X Key Issue #X: <Key Issue Name>

### 2.X.1 Key issue details

### 2.X.2 Security threats

### 2.X.3 Potential security requirements

# 3 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 3.1 Solution #1: 1-Hop Forward Security Solution for LTM

### 3.1.1 Introduction

This solution address key issue #1.

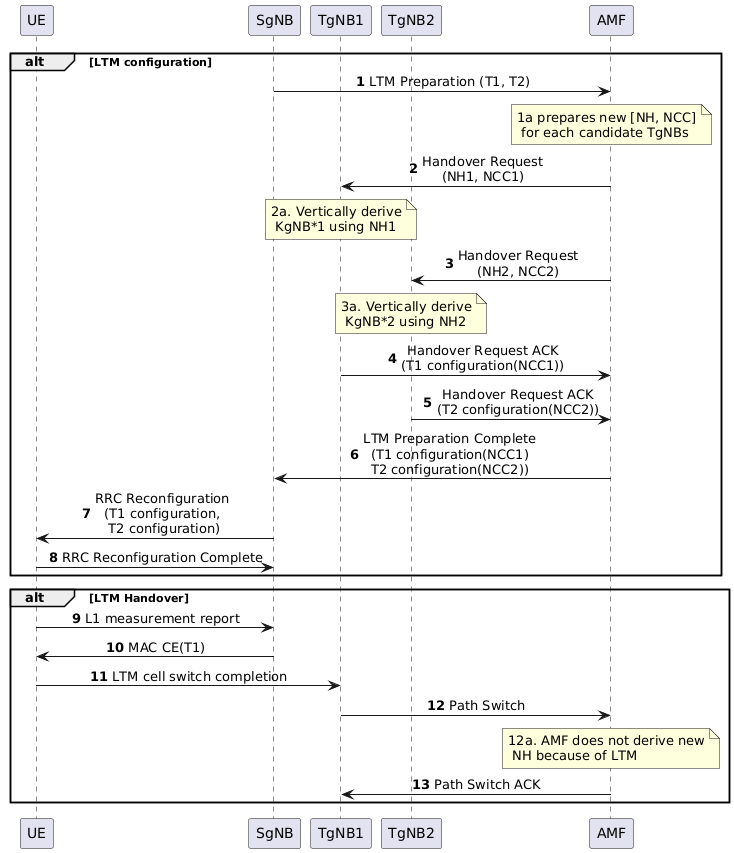
This solution consists of two phases: LTM configuration and LTM handover.

During the LTM configuration phase, the proposal is to utilize an N2 handover-like procedure to prepare a new NH for each candidate TgNBs. This approach allows for the achievement of 1-hop forward security, as the SgNB cannot access TgNB’s KgNB.

In the LTM handover phase, the proposal is to employ an Xn handover-like procedure to trigger a path switch for establishing the N3 path.

### 3.1.2 Solution details

#### 3.1.2.1 Procedure



**Figure 3.1.2-1: Procedure for 1-Hop Forward Security Solution for LTM**

**LTM configuration Phase:**

1. SgNB selects n candidate TgNBs, the max value of n is 6, because at the initial AS security context setup procedure, the second NH (NCC=1) is not used according to 6.9.2.1.1 in TS 33.501 [2], so, there are 7 available NCC values. The candidate TgNBs and SgNB shall be controlled by the same AMF.
2. SgNB sends LTM preparation message to the AMF, the message includes candidate TgNB IDs (e.g. T1, T2).

If there is new Kamf and AS key is not sync yet, the AMF may pause LTM process, and trigger UE context modification procedure. After the procedure, the AMF continues LTM process.

The AMF prepares [NH, NCC] for the candidate TgNBs, i.e. for each TgNB, the AMF derives a new NH, and add NCC by 1.

1. – 3. The AMF sends Handover Request to the candidate TgNBs, the security context (including NH, NCC, UE security capability, UP security policy) is included.

The candidate TgNBs vertically derive KgNB based on received NH, select algorithm and determine the UP activation based on the received security context, and construct LTM configuration including the NCC, the selected algorithm and the UP activation.

1. - 5. The candidate TgNBs reply the Handover Request ACK including the RRC configurations (e.g. T1 configuration, T2 configuration) to the AMF.
2. The AMF sends LTM preparation complete to the SgNB including the LTM configurations.

NOTE: LTM preparation and LTM preparation complete are defined by TR 38.413.

1. The SgNB sends RRC Reconfiguration message to the UE to indicate the LTM configurations.
2. The UE stores the LTM configurations and sends RRC Reconfiguration Complete message to the SgNB. The UE vertically derives KgNBs based on LTM configurations. In this case, 1 hop forward security is achieved.

To be more specific, after receiving n LTM configurations, the UE derives KgNB\* based current NCC and NCC in LTM configurations. After that, the UE makes the largest NCC in LTM configurations as current NCC.

For example, it assumes that UE has current NCC=5 and receives 2 LTM configurations (T1 configuration (NCC=6), T2 configuration (NCC=7)). The UE derives KgNB1\* based on NCC=5 and NCC=6 (NH derivation once), and derives KgNB2\* based on NCC=5 and NCC=7 (NH derivation twice). The UE stores the derived KgNB1\* in T1 configuration and stores the derived KgNB2\* in T2 configuration. After that, the UE makes current NCC=7.

In case that there is candidate cell adding or releasing, the UE will do step 8 again.

For example, based on above example, the UE has current NCC=7, and 2 LTM configurations, it assumes that UE receives 2 LTM configurations (T3 configuration (NCC=0), T4 configuration (NCC=1)) for adding and 1 LTM configuration (T1) for releasing. The UE derives KgNB3\* based on NCC=7 and NCC=0 (NH derivation once), and derives KgNB4\* based on NCC=7 and NCC=1 (NH derivation twice). The UE stores the derived KgNB3\* in T3 configuration and stores the derived KgNB4\* in T4 configuration. The UE deletes T1 configuration. The UE makes current NCC=1.

**LTM handover Phase：**

1. UE performs L1 measurement and reports to the SgNB.
2. The SgNB indicates the UE to perform LTM handover to TgNB1.
3. The UE triggers LTM handover to the TgNB1. The UE applies indicated TgNB’s LTM configuration (e.g. T1 configuration). The UE uses derived KgNB as depicted in step 8 for AS security.
4. The TgNB1 sends Path Switch to the AMF. The AMF does not derive new NH and NCC if the AMF has configured the LTM configurations for the UE.
5. The AMF sends Path Switch ACK to the TgNB1, the Path Switch includes current NH and NCC. The TgNB1 ignores the NH, NCC.

NOTE: Key lifecycle is the same with 6.2.2.3 of this specification.

#### 3.1.2.2 L3 Xn handover

Following step 13, TgNB1 and UE will utilize KgNB\* for AS security, the KgNB\* is derived from NH1 received in step 2. If the UE is to handover to TgNB3, not present in the candidate TgNB list, TgNB1 will derive KgNB\*\* based on KgNB\* using horizontal derivation, as the AMF does not derive a new NH for TgNB1 in step 12. Subsequently, TgNB1 will transmit KgNB\*\* to TgNB3, indicating the UE to trigger handover to TgNB3. TgNB3 will conduct a path switch to obtain a new [NH, NCC] from the AMF, as AMF acknowledges that TgNB3 is not in LTM candidate TgNB list. The process is backward compatible for L3 Xn handover.

### 3.1.3 Evaluation

The solution address key issue #1.

The solution can achieve 1 hop forward security, i.e. gNBs in LTM are unaware of each other's key, and it has no impact on MAC CE. Besides that, it could meet subsequent LTM requirement.

The solution has the following impact:

UE: Minimum impact. The UE derives and stores KgNB\* for each candidate LTM gNBs after receiving RRC Reconfiguration in LTM preparation phase.

SgNB: N2 message enhancement for supporting LTM preparation.

TgNB: Minimum impact. Ignore NH, NCC in Path Switch ACK in case of LTM.

AMF: N2 message enhancement for supporting LTM preparation. New NH, NCC derivation in case of LTM. AS key sync before LTM.

## 3.2 Solution #2: Inter-CU LTM

### 3.2.1 Introduction

This solution describes the Option 4 as described by the RAN document [3] and is referring to the Key Issue 1.

### 3.2.2 Solution details

The inter-CU LTM procedure description will be split into two phases, i.e., first comes the LTM preparation phase and second is the LTM cell switch execution.



**Figure 3.2.2-1: Inter-CU LTM Procedure (overview)**

1. The UE has already connected to the source gNB and is in UE connected state. The AS and NAS security has been activated and are applicable to traffic that is going between UE and Network.

2. The UE (Step 2a) and the AMF (Step 2b) compute the NH at NCC=1 values.

3. The UE is sending measurement report.

4. The source gNB is preparing the LTM cell switch candidates, i.e., is computing keys based on horizontal key derivation and is sharing those keys with target gNB. The horizontal key derivation in this case is preparing for the subsequent handover preparation procedure.

Editor’s Note: The preparation for the subsequent XnP handover preparation is FFS.

5./6. The source gNB is triggering handover preparation procedure over XnAP. The source gNB is sending to every of the candidates the corresponding AS security information (i.e., Key NG\_RAN\* and NCC). The XnAP handover preparation procedure is according to [4]. The sharing of the AS security information will enable the target gNB to run horizontal key derivation at handover unless otherwise requested.

7./8. The source gNB is triggering RRC reconfiguration procedure and is includuding the next NCC value (NCC=1).

Editor’s Note: Evaluation is needed on the lifecycle management for unused NCC value at source gNB.

9. The UE is periodically sending measurements.

10. The source gNB is deciding for inter-CU LTM cell switch and is sending a MAC CE cell switch command to the UE (Step 11).

12. The UE is generating new keys based on NCC indication. Vertical key derivation will be performed.

13. The UE is responding with a reconfiguration complete.

14. The target gNB is sending a NGAP path switch towards the AMF for the generation of a new { NH, NCC } pair.

15. The NGAP path switch procedure is triggering the computing of new { NH, NCC } pair inside the UE and the AMF.

16. void

17./18. The target gNB is now the new source gNB and is therefore computing new keys and is sharing those with the inter-CU candidates. The role and corresponding features of a source gNB is moving to the new source gNB.

19. The new target gNB (former source gNB) is discarding all unused NCC values which have been maintained because of the (former) source gNB role.

20./21. The target gNB is now sending a RRC reconfiguration message that includes the next NCC value (NCC=2). The UE is responding with related complete message.

Editor’s Note: Evaluation is needed for the subsequent LTM in case of an L3 handover.

### 3.2.3 Evaluation

TBD

## 3.3 Solution #3: NCC synchronization solution for LTM

### 3.3.1 Introduction

This solution is for key issue #1. This solution is an enhancement of option 1A where the NCC value is included in the cell switch command MAC CE.

The principle of the solution is:

Upon receiving the NCC value in the cell switch command, the UE compares the received NCC value with the locally stored one.

- If the received NCC value is smaller than the locally kept value, the UE discards the MAC CE and initiates the RRC re-establishment procedure since the message may be tampered.

- If the received NCC value is larger than the locally kept value, the UE synchronizes the NH parameter and computes the KNG-RAN\* as described in the solution details.

- If the received NCC value is the same as the locally kept value, the UE computes the KNG-RAN\* directly using the current parameters.

### 3.3.2 Solution details



**Figure 3.3.2-1: Signalling procedure for inter-CU LTM**

1. The UE sends a *MeasurementReport* message to the gNB. The gNB decides to configure LTM and initiates LTM preparation.
2. The source gNB issues a Handover Request message to one or more candidate cells belonging to one or more candidate gNBs. The Handover Request passing a transparent RRC container with necessary information to prepare the handover at the target side. Keys for the target gNBs are not derived and not sent to the target gNB.

Admission Control may be performed by the target gNB.

1. The target gNB prepares the handover with L1/L2 and sends the HANDOVER REQUEST ACKNOWLEDGE to the source gNB, which includes a transparent container to be sent to the UE as an RRC message to perform the handover.
2. The gNB transmits an *RRCReconfiguration* message to the UE including the LTM candidate configurations. The gNB also includes the NCC into the message.
3. The UE stores the LTM candidate configurations and correspongding NCC, and transmits an *RRCReconfigurationComplete* message to the gNB.
4. The UE performs DL and UL synchronization with the LTM candidate cells as existing procedure.

7. The UE performs L1 measurements on the configured candidate cell(s) and transmits L1 measurement reports to the gNB. L1 measurement should be performed as long as RRC reconfiguration (step 4) is applicable.

8. The gNB decides to execute LTM. The gNB performs vertical key derivation and forward the { KNG-RAN\*, NCC} pair to the target. The target gNB/ng-eNB uses the received KNG-RAN\* directly as KgNB to be used with the UE. The target gNB/ng-eNB associates the NCC value received from source gNB/ng-eNB with the KgNB.

9. The target gNB sends the Key Update Acknowledge to the source gNB.

10. The gNB transmits a MAC CE triggering cell switch by including the candidate configuration index of the target cell. The gNB also includes the NCC in plain text into the message. As soon as the UE receives the NCC, it compares the NCC value with its own NCC (or the NCC value received in Step 4). If it is smaller than the NCC in UE (or the NCC received in Step 4), it indicates that the message may be tampered with and handover is canceled. Then the UE initiates the RRC re-establishment procedure. If the UE received an NCC value that was larger than the NCC associated with the currently active KgNB, the UE shall first synchronize the locally kept NH parameter iteratively and increasing the NCC value until it matches the NCC. When the NCC values match, the UE computes the KNG-RAN\* from the synchronized NH parameter. if the UE received an NCC value that was the same as the NCC associated with the currently active KgNB, the UE computes the KNG-RAN\* directly using the current parameters. The UE switches to the target cell and applies the configuration indicated by candidate configuration index.

NOTE: Whether integrity protection on MAC CE is needed should be considered from the perspective of the whole procedure.

11. The UE performs the random access procedure towards the target cell, if UE does not have valid TA of the target cell.

12. The UE completes the LTM cell switch procedure by sending *RRCReconfigurationComplete* message to target cell. If the UE has performed a RA procedure in step 11 the UE considers that LTM cell switch execution is successfully completed when the random access procedure is successfully completed. For RACH-less LTM, the UE considers that LTM cell switch execution is successfully completed when the UE determines that the network has successfully received its first UL data.

13. Path switch procedure between the target gNB, AMF and UPF.

The steps 6-13 can be performed multiple times for subsequent LTM using the LTM candidate configuration(s) provided in step 4.

Editor’s Note: How to solve the forward security is FFS.

Editor’s Note: How to support AS security context synchronization after path switch is FFS.

Editor’s Note: How to deal with the received NCC value smaller than the locally kept one is FFS.

### 3.3.3 Evaluation

This solution address the security requirements of KI #1.

This solution does not require any new RRC reconfiguration message to be sent between two LTM handovers and therefore meets the requirement of subsequent LTM.

The solution has the following impact:

- The NCC value is included in the cell switch command MAC CE.

Editor’s Note: Further evaluation is FFS

## 3.4 Solution #4: MAC CE based solution to deliver the NCC(s)

### 3.4.1 Introduction

This solution proposes the procedure for LTM key derivation. The legacy handover procedure in TS 33.501 clause 6.9.2 will be reused as much as possible. RAN2 procedures on LTM (no DC) are used as the basis.

### 3.4.2 Details

Pre-assumption:

* In this solution, gNB1, gNB2 and gNB3 are the candidate cells, UE is moving from gNB1 to gNB2, then from gNB2 to gNB3.
* Source gNB1 configures the UE, gNB2 and gNB3 with NCC1 to be used for the key derivation.

A diagram with text and black text

Description automatically generated with medium confidence

**Figure 3.4.2-1: MAC CE based LTM procedure**

Step 0. Source gNB1 configures the UE, gNB2 and gNB3 with NCC1 to be used for the key derivation.

NOTE: Integrity protection on MAC CE is not in the scope of this solution.

Step 1. gNB1 sends the MAC CE to the UE including NCC1(assuming NCC1 is the next NCC to be used for next handover.

Step2. gNB1 derives K\_gNB21 based on NCC1 and sends it to gNB2, the key derivation method follows TS 33.501 Annex A.11.

Step3. gNB1 derives K\_gNB31 based on NCC1 and sends it to gNB3, the key derivation method follows TS 33.501 Annex A.11.

NOTE: the order of step 2/3 and step1 follows RAN2 procedure.

Step4. UE triggers the inter-CU switch, handover from gNB1 to gNB2. UE derives K\_gNB21 using NCC1.

Step5. After the handover, gNB2 sends NGAP PATH SWITCH COMPLETE message to AMF.

Step6. AMF sends the NGAP PATH SWITCH ACK message back to gNB2, including a new pair {NH2, NCC2}.

Step7. gNB2 derives K\_gNB12 based on NCC2 and sends it to gNB1, the key derivation method follows TS 33.501 Annex A.11.

Step8. gNB2 derives K\_gNB32 based on NCC2 and sends it to gNB3, the key derivation method follows TS 33.501 Annex A.11.

Step9. gNB2 sends the MAC CE to the UE including NCC2 to be used for next handover.

NOTE: the order of step 7/8 and step9 follows RAN2 procedure.

Step10. UE triggers the inter-CU switch, handover from gNB2 to gNB3. UE derives K\_gNB32 using NCC2.

Step11. After the handover, gNB3 sends NGAP PATH SWITCH COMPLETE message to AMF.

Step12. AMF sends the NGAP PATH SWITCH ACK message back to gNB3, including a new pair {NH3, NCC3}.

Editor’s Note: AS security context sync-up after path switch is ffs

### 3.4.3 Evaluation

This solution leverages MAC CE to deliver the NCC, which is aligned with RAN2 motivation for LTM feature. The NCC configuration can be carried within LTM Cell Switch Command MAC CE (TS 38.321) without any further impact on the system.

MAC CE has no integrity protection so far, this is a security concern not only to this solution#4, but also to other solutions based on MAC CE.

## 3.5 Solution #5: RRC message based solution to deliver the NCC(s)

### 3.5.1 Introduction

This solution proposes the procedure for LTM key derivation. The legacy handover procedure in TS 33.501 clause 6.9.2 will be reused as much as possible. RAN2 procedures on LTM (no DC) are used as the basis.

### 3.5.2 Details

Pre-assumption:

* In this solution, gNB1, gNB2 and gNB3 are the candidate cells, UE is moving from gNB1 to gNB2, then from gNB2 to gNB3.
* Source gNB1 and UE will use NCC1 for the next switch.

A diagram of a computer program

Description automatically generated

**Figure 3.5.2-1: RRC message based LTM procedure**

Step 0. Source gNB1 configures the UE, NCC1 is the next NCC to be used. gNB1 configures gNB2 and gNB3 as the candidate CUs. Step 1. gNB1 sends the MAC CE to the UE to trigger the switch.

Step2. gNB1 derives K\_gNB21 based on NCC1 and sends it to gNB2, the key derivation method follows TS 33.501 Annex A.11.

Step3. gNB1 derives K\_gNB31 based on NCC1 and sends it to gNB3, the key derivation method follows TS 33.501 Annex A.11.

NOTE 1: the order of step 2/3 and step1 follows RAN2 procedure.

Step4. UE performs the inter-CU switch, handover from gNB1 to gNB2. UE derives K\_gNB21 using NCC1.

Step5. After the handover, gNB2 sends NGAP PATH SWITCH COMPLETE message to AMF.

Step6. AMF sends the NGAP PATH SWITCH ACK message back to gNB2, including a new pair {NH2, NCC2}.

Step7. gNB2 sends RRC message including the NCC2 to UE to be used for next switch.

NOTE 2: which RRC message to be used is based on RAN2 decision.

Step8. gNB2 derives K\_gNB12 based on NCC2 and sends it to gNB1, the key derivation method follows TS 33.501 Annex A.11.

Step9. gNB2 derives K\_gNB32 based on NCC2 and sends it to gNB3, the key derivation method follows TS 33.501 Annex A.11.

NOTE 3: the order of step 8/9 and step7 follows RAN2 procedure.

Step10. gNB2 sends the MAC CE to the UE to trigger the switch.

Step11. UE performs the inter-CU switch, handover from gNB2 to gNB3. UE derives K\_gNB32 using NCC2.

Step12. After the handover, gNB3 sends NGAP PATH SWITCH COMPLETE message to AMF.

Step13. AMF sends the NGAP PATH SWITCH ACK message back to gNB3, including a new pair {NH3, NCC3}.

Step14. gNB3 sends RRC message including the NCC3 to UE to be used for next switch.

Editor’s Note: how to support AS re-keying is FFS.

### 3.5.3 Evaluation

This solution leverages RRC message to deliver NCC, which provides security protection.

## 3.6 Solution #6: Key handling during LTM

### 3.6.1 Introduction

This solution resolves key issue #1. During inter-CU LTM procedure, security key handling is required like other mobility procedures supported. Horizontal and vertical key derivation also need to be supported and applied for inter-CU LTM procedure.

This solution supports security handling for LTM by supporting both horizontal and vertical key derivations. During LTM execution, NCC value can be provided to other gNB(s) for later subsequent LTM. The solution also shows two methods to synchronize updated NCC value between the UE and the gNB via RRC message (RRC Reconfiguration) or MAC CE (LTM Cell Switch Command). If NCC value needs to be sent before subsequent LTM, RRC Reconfiguration can be sent to the UE right after the LTM execution. Otherwise, Cell Switch Command includes the NCC value and can be sent to the UE during subsequent LTM. To hide NCC value in the MAC CE message, the NCC value can be included in indirect ways.

### 3.6.2 Solution details



**Figure 3.6.2-1: Procedure of LTM with key handling**

The steps shown in Figure 3.6.2-1 is described as below:

1. UE is in state of RRC\_CONNECTED.
2. The UE sends a Measurement Report message to the source gNB when configured measurement conditions met.
3. The source gNB decides to configure LTM and initiates LTM preparation. The source gNB derives new KgNB\* for each candidate cell for target gNB(s).
4. The source gNB sends Handover Request including newly derived KgNB\* and NCC to the target gNB.
5. The target gNB sends Handover Request Acknowledge to the source gNB including the NCC value received from the source gNB.
6. The UE receives RRC Reconfiguration message and configures candidates cell configuration to access later.
7. The UE responses RRC Reconfiguration Complete message to the source gNB.
8. The UE sends a Measurement Report message to the source gNB again. The source gNB decides to initiate LTM execution.
9. The source gNB sends LTM Cell Switch Command over MAC CE to the UE. When the UE receives LTM Cell switch command, the UE derives new KgNB\*\* for the cell of the target gNB.
10. The source gNB informs Cell Switch Notification to the target gNB.
11. The UE may perform RACH and access the indicated cell of the target gNB.
12. If cell switch succeeded, the UE sends RRC Reconfiguration Complete to the target gNB.
13. The target gNB sends Path Switch Request to the AMF.

If horizontal derivation is preferred, the target gNB can include information that indicates horizontal key derivation during LTM procedure in the message towards the AMF. In this case, the AMF doesn’t compute new NH and increase NCC. Step 15 will be skipped. In step 17, LTM Cell Switch doesn’t include NCC value.

If vertical key derivation is preferred, the target gNB doesn’t inform any key derivation indicator to the AMF. In this case, the AMF computes new NH and increases NCC.

1. The AMF responses Path Switch Request ACK to the target gNB. If horizontal key derivation is decided in the step 12, non-computed NH and non-increased NCC can be included in the message. If vertical key derivation is decided in the step 12, newly computed NH and increased NCC are included in the message.

If NGAP PATH SWITCH REQUEST ACKNOWLEDGE message contains NSCI (New Security Context Indicator) or difference security capabilities, Intra-gNB-CU handover will be performed immediately after the LTM execution. Updated security key information can be delivered to candidate cells in other gNBs during the intra-gNB-CU handover. In this case, currently ongoing LTM procedure can be aborted.

1. The target gNB further provides newly derived keys to candidate cells of other gNBs for subsequent LTM operations.
2. The target gNB may send RRC Reconfiguration including NCC to inform to the UE. Consequently, the UE may response RRC Reconfiguration Complete. If target gNB doesn’t send RRC reconfiguration with NCC, providing NCC to the UE can be performed in the step 17.

NOTE: Operator can choose a method to sync NCC between the UE and the gNB. (e.g. by sending RRC Reconfiguration, LTM Cell Switch (MAC CE) with NCC)

NOTE: The target gNB becomes the source gNB and prepares subsequent LTM operations.

1. The UE sends Measurement Report to the current source gNB for subsequent LTM.
2. The current source gNB sends LTM Cell Switch Command over MAC CE to the UE. If the step 15 was not performed, NCC can be included in the message. The NCC value may be delivered to the UE in indeirct way. (e.g. using index of NCC value, or using special equation)
3. Perform the remaining LTM procedure following the step 9 to 15.

### 3.6.3 Evaluation

This solution addresses Key Issue #1.

This solution supports both vertical and horizontal key derivation for LTM procedure. If horizontal key derivation is preferred by operator, NCC value doesn’t need to be shared to the UE since the NCC was not increased. If vertical key derivation is preferred, updated NCC can be delivered to the UE by sending additional RRC Reconfiguration after LTM execution or LTM Cell Switch Command (MAC CE) during subsequent LTM procedure.

The solution has impact on UE, gNB and AMF:

Updated NCC value in RRC Reconfiguration or LTM Cell Switch Command (MAC CE) will impact to UE and gNB.

Updating security key information to candidate cells of other gNBs at the end of step in LTM execution phase will impact to gNB.

An indicator to lead to horizotnal key derivation in NGAP PATH SWITCH REQUEST to AMF will impact to gNB and AMF.

## 3.7 Solution #7: Security for Inter-gNB LTM procedure

### 3.7.1 Introduction

This solution addresses the security requirement of key issue#1. In this solution, it is proposed that for LTM cell switch the KNG-RAN\* is derived from the current KgNB (i.e., horizontal key derivation) or from a fresh and unused pair of {NCC, NH}, if available (i.e., vertical key derivation) in the source gNB.

Once the source gBN decides on the LTM cell switch, the source gNB computes KNG-RAN\* from target PCI, its frequency ARFCN-DL/EARFCN-DL, and either from currently active KgNB or from the NH as described in Annex A.11/A.12 of TS 33.501 [2]. The source gNB performs a vertical key derivation in case it has an unused {NH, NCC} pair. Then the source gNB forwards the {KNG-RAN\*, NCC} pair to the target gNB in the CELL SWITCH NOTIFICATION message to the target gNB. That is, the source gNB distributes the key during the LTM cell switch execution phase. The target gNB uses the received KNG-RAN\* directly as KgNB with the UE. The target gNB associate the NCC value received from source gNB with the KgNB.

After the radio link handover, whenever the gNB receives a fresh pair of {NCC, NH} from the AMF, the gNB sends the NCC value of the received fresh pair (NCCLTM) and the *keySetChangeIndicator* to the UE in a protected RRC message (can be a new RRC message (RRC LTM Security Context). If the gNB received NSCI along with the fresh pair of {NCC, NH} from the AMF, then the gNB set the value of *keySetChangeIndicator* field to true and send it along with the NCCLTM in the RRC message. The UE stores the received NCCLTM value and the *keySetChangeIndicator*.

Upon receiving the Cell Switch Command from the source gNB,

- if the NCC of the current KgNB is less than the stored NCCLTM value, then the UE synchronize the locally kept NH parameter by computing the function defined in Annex A.10 iteratively as specified in TS 33.501 [2] and computes the KNG-RAN\* from the synchronized NH parameter.

- if the NCCLTM is equal to the NCC value associated with the current KgNB, then the UE uses the active KgNB to derive the KNG-RAN\*.

### 3.7.2 Solution details



**Figure 3.7.2-1: Inter-gNB LTM procedure**

1. The UE sends a *MeasurementReport* message (L3 measurement result) to the source gNB.

2. The source gNB determines to initiate inter-gNB LTM configuration.

3. The source gNB sends a HANDOVER REQUEST message to the candidate gNB(s) for each candidate cell to request LTM configurations, which carries a LTM indicator and other related LTM information.

4. Admission Control may be performed by the target gNB.

5. The candidate gNB sends LTM response message (HANDOVER REQUEST ACKNOWLEDGE) including configuration of LTM candidate cell(s) to the source gNB. The LTM response message is sent for each candidate cell.

6. The source gNB transmits an *RRCReconfiguration* message to the UE including the LTM candidate configurations.

7. The UE stores the LTM candidate configurations and transmits an *RRCReconfigurationComplete* message to the gNB.

8. Early synchronization to the target candidate cell(s) may be performed as specified in TS 38.300 [1].

9. The candidate gNB forwards the TA value and the associated information to source gNB via an XnAP signaling.

10. The UE sends the L1 measurement result to the source gNB.

11. The source gNB decides to execute LTM to a candidate target cell. The source gNB generates the KNG-RAN\* from target PCI, its frequency ARFCN-DL/EARFCN-DL, and either from currently active KgNB or from the NH as described in Annex A.11/A.12 of TS 33.501 [2]. The source gNB performs a vertical key derivation in case it has an unused {NH, NCC} pair and if NCCLTM and the keySetChangeIndicator are provided to the UE (c.f., Step 21). Horizontal key derivation is performed, if the unused NCCLTM value is not successfully provided to the UE.

12. The source gNB sends the Cell Switch command to the UE via MAC CE. Upon receiving the cell switch command, if the NCC of the current KgNB is less than the stored NCCLTM value, then the UE synchronize the locally kept NH parameter by computing the function defined in Annex A.10 iteratively as specified in TS 33.501 [2] and computes the KNG-RAN\* from the synchronized NH parameter. If the NCCLTM is equal to the NCC value associated with the current KgNB, then the UE uses the active KgNB to derive the KNG-RAN\*.

13. The source gNB sends the CELL SWITCH NOTIFICATION message to target gNB via an XnAP signaling. In this notification message the source gNB includes the generated {KNG-RAN\*, NCC} pair to the target gNB.

NOTE 1: Steps 12 and 13 are performed in parallel, so that the target gNB gets the {KNG-RAN\*, NCC} before step 15.

14. The target gNB detects the UE access as specified in TS 38.300 [1]. Upon receiving the KNG-RAN\* from the source gNB, the target gNB uses the received KNG-RAN\* directly as KgNB to be used with the UE. The target gNB associates the NCC value if received from source gNB with the KgNB.

15. The UE sends an *RRCReconfigurationComplete* message to the target gNB.

16. The target gNB sends the HANDOVER SUCCESS message to the source gNB to inform that the UE has successfully accessed the target cell.

17. The source gNB sends the SN STATUS TRANSFER message for the late data forwarding following the principles described in step 7 of Intra-AMF/UPF Handover in clause 9.2.3.2.1 in TS 38.300 [1].

NOTE 2: Late data forwarding may be initiated as soon as the source gNB sends the Cell Switch command to the UE via MAC CE in step 12.

18. The target gNB sends a PATH SWITCH REQUEST message to 5GC (AMF) to trigger 5GC to switch the DL data path towards the target gNB and to establish an NG-C interface instance towards the target gNB.

19. The 5GC (AMF) confirms the PATH SWITCH REQUEST message with the PATH SWITCH REQUEST ACKNOWLEDGE message to target gNB. The AMF sends the newly computed {NH, NCC} pair to the target gNB in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The sent NGAP PATH SWITCH REQUEST ACKNOWLEDGE message in addition may contain a NSCI (New Security Context Indicator), as specified in TS 33.501 [2].

20. Upon reception of the PATH SWITCH REQUEST ACKNOWLEDGE message from the 5GC (AMF), the target gNB stores the received {NH, NCC} pair for further handovers and may send the UE CONTEXT RELEASE to inform the source gNB about the success of the handover. The source gNB may then release radio and C-plane related resources associated to the UE context. Any ongoing data forwarding may continue.

21. Whenever the gNB receives a fresh pair of {NCC, NH} from the AMF, the gNB sends the NCC value of the received fresh pair (NCCLTM) and the *keySetChangeIndicator* to the UE in a protected RRC message (can be a new RRC message (RRC Security Configuration Request). If the gNB received NSCI along with the fresh pair of {NCC, NH} from the AMF, then the gNB set the value of *keySetChangeIndicator* field to true and send it along with the NCCLTM in the RRC message.

22. The UE stores the received NCCLTM value and the *keySetChangeIndicator* to generate the appropriate KNG-RAN\* for the LTM Cell Switch procedure.

For subsequent LTM procedures, steps 10 to 22 are performed.

### 3.7.3 Evaluation

This solution addresses the security requirement of key issue#1.

Solution supports both vertical and horizontal key derivation for LTM cell switch procedure.

With the indication of the NCCLTM value and the *keySetChangeIndicator* from the gNB to the UE, the UE appropriately generates the KNG-RAN\* even if RRC state transition and/or Intra-gNB-CU handovers are performed before LTM cell switch.

## 3.8 Solution #8: Rekeying synchronization at handover completion

### 3.8.1 Introduction

Among the multiple options discussed for rekeying synchronization for inter-CU LTM feature, option 4 uses RRC signalling to deliver the NCC value to the UE after each inter-CU LTM cell switch execution, which ensures the NCC value is protected. The NCC value received in handover completion phase is used for key derivation at the next LTM cell switch execution. This solution details the rekeying synchronization for this option.

According to the enhancement of inter-gNB LTM, RRC configuration of the candidate gNBs can be preconfigured on the UE by the initial gNB in LTM preparation phase. This solution proposes that the initial gNB configures a NCC value on the UE via RRC reconfiguration signaling in LTM preparation phase. The configured NCC value is used for the next inter-CU LTM handover from the initial gNB to the target gNB (i.e. one of the candidate gNBs). In each handover completion phase, after the target gNB receives the new pair of {NH, NCC} from the AMF, it sends the new NCC value to the UE via RRC reconfiguration signalling.

In this way, to the end of each inter-CU LTM handover, both the UE and the gNB (e.g. gNB1 handed over from gNB0) can obtain the updated NCC value for rekeying synchronization for the next handover (e.g. from gNB1 to gNB2).

As part of AS security context, AS security algorithms are also negotiated between the UE and each of the candidate gNBs in LTM preparation phase. The UP security policy associated with the active PDU session is also sent by the source gNB to the candidate gNBs in LTM preparation phase.

### 3.8.2 Solution details

The procedure below comprises LTM preparation phase, LTM execution phase, LTM completion phase, subsequent LTM execution phase, subsequent LTM completion phase.



**Figure 3.8.2.1: NCC Delivery via RRC Signalling**

1. A connected UE sends RRC measurement report to the serving/source gNB0.

2. The serving/source gNB0 decides to do LTM preparation for candidate gNBs.

3. The serving/source gNB0 sends Handover Request to each of the candidate gNBs, which includes the UE security capabilities and the UP security policy associated with the active PDU session (e.g. session 1) of the UE.

4. Each of the candidate gNBs selects the AS security algorithms to be used for AS security with the UE, and then stores the selected AS security algorithms in the LTM configuration to be sent to the UE.

Each of the candidate gNBs also stores the received UP security policy associated with the active PDU session (e.g. session 1).

5. Each of the candidate gNBs returns the LTM configuration to the serving/source UE via Handover Request Acknowledge.

6. The serving/source gNB0 sends the LTM configuration of the candidate gNBs to the UE. The serving/source gNB0 also includes NCC1 and keySetChangeIndicator in the RRC reconfiguration message. If gNB0 is the initial gNB that the UE camps on, the configured NCC value NCC1=0. If the UE was handed over to gNB0 from another gNB previously, the NCC value should already be synchronized between the UE and gNB0.

7. While the UE is moving, the UE sends L1 measurement report to the serving/source gNB0.

8. Once selecting the target gNB (candidate gNB1), the serving/source gNB0 determines whether LTM procedure needs to be triggered. If the serving/source gNB0 does not have any unused NH, it performs horizonal key derivation by deriving KNG-RAN\* from KgNB0. If the serving/source gNB0 has an unused NH1 (associated with NCC1), it performs vertical key derivation by deriving KNG-RAN\* from NH1.

9. The serving/source gNB0 sends the derived KNG-RAN\* and the NCC1 used for KNG-RAN\* derivation to gNB1. The gNB1 takes KNG-RAN\* as KgNB1 and returns the NCC1 to the serving/source gNB0.

10. The serving/source gNB0 sends the MAC CE command to the UE.

11. Upon receiving the MAC CE from the serving/source gNB0,

11a. The UE first checks the keySetChangeIndicator to determine weather a new KgNB needs to be derived.

11b. If no new KgNB needs to be derived, the UE compares the NCC1 received from gNB0 at step #6 with the NCC associated with the current KgNB. If the former is identical to the latter, the UE performs horizonal key derivation. If the former is greater than the latter, the UE performs vertical key derivation by deriving NH1 corresponding to NCC1 and then KNG-RAN\*.

11c. The UE detaches from the serving/source gNB0 and applies the configuration of the target gNB (gNB1), taking KNG-RAN\* as KgNB1 to be used with the gNB1.

12~14. LTM handover is completed after Path Switch procedure with the AMF. A new pair of NH and NCC (NH2, NCC2) is generated by the AMF and delivered to gNB1, of which the new NCC value (NCC2) and corresponding ketSetChangeIndicator are sent to the UE via RRC Reconfiguration. The UE stores the NCC2 and the ketSetChangeIndicator to be used in the subsequent LTM handover.

15. The user data of PDU session 1 is switched from gNB0 to gNB1, which applies the UP security policy received from gNB0 in LTM preparation phase.

16. While connecting to the gNB1, the UE e.g. releases PDU session 1 and establishes a new PDU session (e.g. session 2) via gNB1, which receives the new UP security policy associated with PDU session 2 from the core network.

17. Upon new UP security activation, the gNB1 may decide to perform LTM candidate preparation.

18. The gNB1 sends the UP security policy associated with the active PDU session 2 via Handover Request to the candidate gNB (gNB2). The gNB2 stores the received UP security policy and returns its updated LTM configuration to gNB1 via Handover Request Acknowledge.

19. The gNB1 forwards the updated LTM configuration of the candidate gNB2 to the UE.

20~24. LTM handover is executed with synchronized rekeying based on NCC2 and corresponding ketSetChangeIndicator for the UE to be handed over to gNB2.

25~27. LTM handover is completed after Path Switch procedure with the AMF. A new pair of NH and NCC (NH3, NCC3) is generated by the AMF and delivered to gNB2, of which the new NCC value (NCC3) and corresponding ketSetChangeIndicator are sent to the UE via RRC Reconfiguration. The UE stores the NCC3 and the ketSetChangeIndicator to be used in the subsequent LTM handover.

28. The user data of PDU session 2 are switched from gNB1 to gNB2, which applies the UP security policy received from gNB1 in step #18.

### 3.8.3 Evaluation

This solution addresses the security requirement of key issue#1.

The solution is applicable for subsequent LTM handover procedure and supports both vertical and horizontal key derivation for LTM cell switch procedure.

This solution ensures that the full AS security context can be synchornized during LTM handover procedure, including the AS security keys, selected AS security algorithms and UP security policy associated with the active PDU session of the UE in handover.

The synchronization of AS security context does not induce additional RRC signalling in LTM execution phase, hence does not delay LTM handover. The solution does not introduce additional signalling in LTM preparation phase, in which all necessary information for AS security context is embedded in LTM preparation configurations. The solution requires additional RRC signalling in LTM completion phase.

This solution does not have any impact on the AMF. The UE and gNB are mainly impacted in LTM completion phase.

In this solution, as the parameters for rekeying synchronization (e.g. updated NCC value) are obtained by the UE before inter-CU LTM handover other than during LTM handover, there is still the possibility that the NCC value used by the UE for LTM handover is not identical to the NCC value used by the serving gNB for LTM handover. Hence the handover failure probability may increase.

3.9 Solution #9: Fixing the RRC/PDCP anchors at inter gNB cell switches

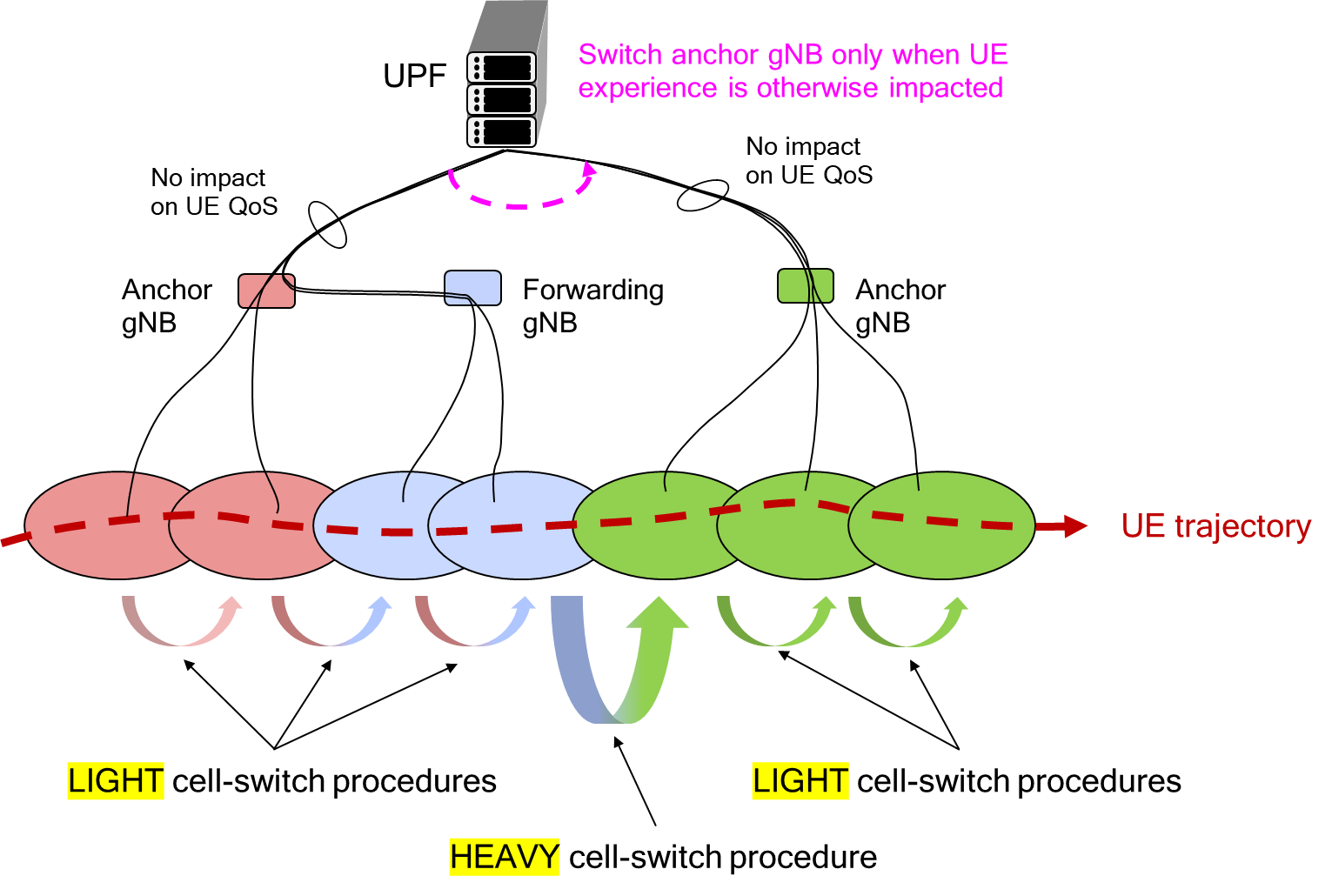
3.9.1 Introduction

This solution proposes to perform inter-gNB LTM with no change of RRC/PDCP anchor.

The reason for this is that there will be no need to change the UE to gNB keys as the handover is not moving the UE to gNB security termination point to a different node. This results in no need to specify new security related signalling for inter-gNB LTM cell switches.

3.9.2 Solution details

As stated above the gain for this solution is keep the RRC/PDCP anchors at a gNB when handing over to the lower layer different which removes the needs for changing the UE to gNB keys at an inter gNB LTM cell switches (as both the control plane and u-plane security termination points are not changing). The benefit of this is illustrated in figure 3.9.2-1.



**Figure 3.9.2-1: Cell switches showing advantage of no RRC/PDCP anchor change at inter-gNB LTM cell switch**

The first and last 3 cell switches are light as they require no change of RRC/PDCP anchor while the middle cell switch is heavy as it requires an RRC/PDCP switch that is required to effectively serve the UE. From a security perspective this solution would work with existing layer 3 handovers as each cell switch is acting like an intra-CU LTM cell switch in that the RRC/PDCP anchor does not change.

Figure 3.9.2-2 provides an example of how the RRC and UP connections of a UE changes as a UE performs multiple inter-gNB LTM cell switches without moving the RRC/PDCP anchor.

A computer screen shot of a diagram

Description automatically generated

**Figure 3.9.2-2: Example of multiple inter-gNB cell switches without RRC/PDCP anchor change**

From a security perspective one advantage of such a solution is there is no need to define new signalling for the UE to gNB security as the security anchor will not changes. Furthermore there is no need to define new security for inter network entity signalling as this will use existing interfaces.

Editor’s Note: The decision of the feasibility of such a solution is left to the RAN working groups, i.e. SA3 cannot unilaterally decide that this solution is way forward for Rel-19.

3.9.3 Evaluation

TBD

## 3.Y Solution #Y: <Solution Name>

### 3.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 3.Y.2 Solution details

### 3.Y.3 Evaluation

Editor’s Note: This clause should at least describe the impact on the system.

# X Overall summary

In total, there are 9 solutions addressing key issue #1. This clause gives an overall mapping between the solutions and technical directions.

Solution #1 utilizes an N2 handover-like procedure to prepare a new NH for each candidate Target gNBs during the LTM configuration phase.

Solutions #2 and #5 to #8 describe the Option 4 as described in [3]. RRC message (e.g., RRC reconfiguration message) is required to configure the next NCC value to UE side.

Solutions #3, #4 and #6 describe the Option 1 as described in [3], where the NCC value is included in the cell switch command MAC CE.

Solution #9 proposes to perform inter-gNB LTM with no change of RRC/PDCP anchor.

# 4 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for the draftCR.