**3GPP TSG-SA3 Meeting #114e *ad-hoc S3-240059***

Electronic meeting, online, 22 - 26 January 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **0059** | **rev** | **-** | **Current version:** | **18.2.0** |  |
|  |
| *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:***  | Test case update to TS 33.511 |
|  |  |
| ***Source to WG:*** | Huawei; HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  SCAS\_5G\_Ph3 |  | ***Date:*** | 2024-01-22 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-18 |
|  | *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 canbe 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:*** | Intra-cell handover is not clear to the tester. The link to the actual procedure needs to explain to the tester.A new example can be used to prove the DRB ID is updated. |
|  |  |
| ***Summary of change:*** | Add a NOTE to explain the procedure of Intra-cell handover.Add a new example, and update the evidance clause. Because the procedures are examples in previous clauses and which one is used can be determined by the test lab. |
|  |  |
| ***Consequences if not approved:*** | Current description is not accurate. |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.13, 4.2.2.1.18 |
|  |  |
|  | **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:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

 \*\*\*\*\*\*\*\*\*\*\*\*\* 1st of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.13 Key refresh at the gNB

*Requirement Name*: Key refresh at the gNB

*Requirement Reference:* TS 33.501 [2], clause 6.9.4.1; TS 38.331 [6], clause 5.3.1.2

*Requirement Description*: Key refresh is possible for KgNB, KRRC-enc, KRRC-int, KUP-enc, and KUP-int (if available), and is to be initiated by the gNB/ng-eNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same KgNB. as specified in TS 33.501 [2], clause 6.9.4.1.

The network is responsible for avoiding reuse of the COUNT with the same RB identity and with the same key, e.g. due to the transfer of large volumes of data, release and establishment of new RBs, and multiple termination point changes for RLC-UM bearers and multiple termination point changes for RLC-AM bearer with SN terminated PDCP re-establishment (COUNT reset) due to SN only full configuration whilst the key stream inputs (i.e. bearer ID, security key) at MN have not been updated. In order to avoid such re-use, the network e.g. uses different RB identities for RB establishments, change the AS security key, or an RRC\_CONNECTED to RRC\_IDLE/RRC\_INACTIVE and then to RRC\_CONNECTED transition as specified in TS 38.331 [6], clause 5.3.1.2.

*Threat References*: TR 33.926 [5], clause D.2.2.7 Key Reuse

*Test Case :*

**Test Name:** TC\_GNB\_KEY\_REFRESH\_DRB\_ID

**Purpose:**

Verify that the gNB performs KgNB refresh when DRB-IDs are about to be reused under the following conditions:

- the successive Radio Bearer establishment uses the same RB identity while the PDCP COUNT is reset to 0, or

- the PDCP COUNT is reset to 0 but the RB identity is increased after multiple calls and wraps around.

**Pre-Conditions:**

The UE, AMF and SMF may be simulated.

**Execution Steps**

1) The gNB sends the AS Security Mode Command message to the UE.

2) The UE responds with the AS Security Mode Complete message.

3) A DRB is set up.

4) DRB is set up and torn down for multiple times within one active radio connection without the UE going to idle (e.g. by the UE making multiple IMS calls, or by the SMF requesting PDU session modification and deactivation via the AMF), until the DRB ID is reused.

**Expected Results:**

Before DRB ID reuse, the gNB takes a new KgNB into use by e.g. triggering an intra-cell handover or triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED.

NOTE：Random Access Procedure defined in clause 9.2.6 of TS 38.300[8] runs in the above procedures.

**Expected format of evidence:**

Part of log that shows all the DRB identities and the corresponding procedure . This part can be presented, for example, as a screenshot.

\*\*\*\*\*\*\*\*\*\*\*\*\* End 1st of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

 \*\*\*\*\*\*\*\*\*\*\*\*\* 2nd of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.18 Key update at the gNB on dual connectivity

*Requirement Name*: Key update at the gNB on dual connectivity

*Requirement Reference:* TS 33.501 [2], clause 6.10.2.1; clause 6.10.2.2.1;clause 6.10.3.1.

*Requirement Description*: When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN is expected to, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last KSN change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN is expected to increment the SN Counter and compute a fresh KSN, and then is expected to perform a SN Modification procedure to update the KSN as specified in TS 33.501 [2], clause 6.10.2.1.

The MN is expected to refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. Refreshing the root key is done using intra cell handover as described in subclause 6.7.3.3 of TS 33.501 [2]. When the root key is refreshed, the SN Counter is reset to '0' as defined above. in that same clause; as specified in TS 33.501 [2], clause 6.10.3.1.

NOTE: The following testcases are only tested when the NR-NR DC, NE-DC and EN-DC scenarios are deployed.

*Threat References*: TR 33.926 [5], clause D.2.2.7 Key Reuse

*Test Case 1:*

**Test Name:** TC\_GNB\_DC\_KEY\_UPDATE\_DRB\_ID

**Purpose:**

Verify that the gNB under test acting as a Master Node (MN) performs KSN update when DRB-IDs are about to be reused.

**Pre-Conditions:**

- Test environment with a gNB or ng-eNB acting as the Secondary Node (SN), which may be simulated

- Test environment with a UE, SMF and AMF, which may be simulated

**Execution Steps**

1. The gNB under test establishes RRC connection and AS security context with the UE.

2. The gNB under test establishes security context between the UE and the SN for the given AS security context shared between the gNB under test and the UE; and generates a KSN sent to the SN.

3. A SCG bearer is set up between the UE and the SN.

4. The gNB under test is triggered to execute the SN Modification procedure to provide additional available DRB IDs to be used for SN terminated bearers (e.g. by the UE making multiple IMS calls, or by the SMF requesting PDU session modification and deactivation via the AMF), until the DRB IDs are reused.

**Expected Results:**

- Before DRB ID reuse, the gNB under test generates a new KSN and sends it via the SN Modification Request message to the SN.

**Expected format of evidence:**

Evidence suitable for the interface, e.g. text representation of the captured SN Modification Request message.

*Test Case 2*:

**Test Name: TC\_GNB\_DC\_KEY\_UPDATE\_SN\_COUNTER**

**Purpose:**

Verify that the gNB under test acting as a Master Node (MN) performs KNG-RAN( AS root key) update when SN COUNTER is about to wrap around.

**Pre-Conditions:**

- Test environment with a gNB or ng-eNB acting as the Secondary Node (SN), which may be simulated

- Test environment with a UE, SMF and AMF, which may be simulated.

**Execution Steps**

1. The gNB under test establishes RRC connection and AS security context with the UE.

2. The gNB under test establishes security context between the UE and the SN for the given AS security context shared between the gNB under test and the UE; and generates a KSN sent to the SN and increases the value of SN Counter.

3. A SCG bearer is set up between the UE and the SN.

4. The gNB under test is triggered to execute the SN Modification procedure to provide updated KSN to SN, until the SN Counter value wraps around.

**Expected Results:**

- Before SN Counter wraps around, the gNB under test takes a new KNG-RAN into use by e.g. triggering an intra-cell handover or triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED.

NOTE：Random Access Procedure defined in clause 9.2.6 of TS 38.300[8] runs in the above procedures.

**Expected format of evidence:**

Part of log that shows the SN Counter values before and after wrapping around and the corresponding procedure. This part can be presented, for example, as a screenshot.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change\*\*\*\*\*\*\*\*\*\*\*\*\*