**3GPP TSG-SA3 Meeting #108-e  *draft\_S3-221888-r1***

**e-meeting, 22 – 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | 0031 | **rev** | **-** | **Current version:** | **17.1.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **x** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Adding a test case for gNB in TS 33.511 clause 4.2.2.1.4 |
|  |  |
| ***Source to WG:*** | ZTE,Keysight |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G |  | ***Date:*** | 2022-08-09 |
|  |  |  |  |  |
| ***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:*** | As specified in TS 33.501 clause 6.8.2.1.3, when the UE decides to resume the RRC connection to transit from RRC\_INACTIVE to RRC\_CONNECTED, the UE sends RRCResumeRequest message on SRB0 and hence it is not integrity protected. However, the RRCResumeRequest message shall include the I-RNTI and a ResumeMAC-I/shortResumeMAC-I.And the source gNB/ng-eNB verifies the ResumeMAC-I/shortResumeMAC-I using the current KRRCint key stored in the retrieved UE 5G AS security context (calculating the ResumeMAC-I/shortResumeMAC-I in the same way as described above). S3-221891 (CR 1441) proposed to add some clarification on the ResumeMAC-I/shortResumeMAC-I check failed. |
|  |  |
| ***Summary of change:*** | gNB should be able to verify the ResumeMAC-I/shortResumeMAC-I correctly. |
|  |  |
| ***Consequences if not approved:*** | uncompleted specification. |
|  |  |
| ***Clauses affected:*** |  4.2.2.1.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS33.501 ... CR1441 ...  |
| ***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 CHANGE \*\*\*

#####  4.2.2.1.4 RRC integrity check failure

*Requirement Name*: RRC integrity check failure

*Requirement Reference:* TS 33.501 [2], clause 6.5.1,clause 6.8.2.1.3.

*Requirement Description*: *"The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side."* as specified in TS 33.501 [2], clause 6.5.1.

“*When the UE decides to resume the RRC connection to transit from RRC\_INACTIVE to RRC\_CONNECTED, the UE sends RRCResumeRequest message on SRB0 and hence it is not integrity protected. However, the RRCResumeRequest message shall include the I-RNTI and a ResumeMAC-I/shortResumeMAC-I.*

*...*

*The source gNB/ng-eNB verifies the ResumeMAC-I/shortResumeMAC-I using the current KRRCint key stored in the retrieved UE 5G AS security context (calculating the ResumeMAC-I/shortResumeMAC-I in the same way as described above).*”as specified in TS 33.501 [2], clause 6.8.2.1.3.

*Threat References*: TR 33.926 [4], clause D.2.2.2, Control plane data integrity protection

*Test Case 1*:

**Purpose:**

Verify that RRC integrity check failure is handled correctly by the gNB.

**Pre-Conditions:**

Test environment with a UE. The UE may be simulated. RRC integrity protection is activated at the gNB.

**Execution Steps**

1a) The UE sends a RRC message to the gNB without MAC-I; or

1b) The UE sends a RRC message to the gNB with a wrong MAC-I.

2b) The gNB verifies the integrity of the RRC message from the UE.

**Expected Results:**

The RRC message is discarded by the gNB after step 1a) or after step 2b).

**Expected format of evidence:**

Sample copies of the log files.

*Test Case 2*:

**Test Name:** TC-RRCResume-INT-gNB

**Purpose:**

Verify that RRCResumeRequest integrity check failure is handled correctly by the gNB.

**Pre-Conditions:**

Test environment with a UE. The UE may be simulated. gNB send RRCRelease message with “suspendConfig” indication. UE enters the Inactive state after receiving RRCRelease message.Then UE recovers from Inactive state to Connected state.

**Execution Steps**

1a) The UE sends a RRCResumeRequest message to the gNB without ResumeMAC-I/shortResumeMAC-I; or

1b) The UE sends a RRCResumeRequest message to the gNB with a wrong ResumeMAC-I/shortResumeMAC-I.

2b) The gNB verifies the integrity of ResumeMAC-I/shortResumeMAC-I from the UE.

**Expected Results:**

There are two ways of execution, when step 1a) is executed, the RRCResumeRequest message is discarded by the gNB after step 1a), when step 1b)is executed, the RRCResumeRequest message is discarded by the gNB after step 2b).

**Expected format of evidence:**

Evidence suitable for the interface e.g. Screenshot containing the operational results.

\*\*\* END OF CHANGES \*\*\*