**3GPP TSG-SA3 Meeting #108-e  *draft\_S3-221891-r1***

**e-meeting, 22 – 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1441** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  |
| *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:***  | Clarification on ResumeMAC-I/shortResumeMAC-I check failed in clause 6.8.2.1.3 |
|  |  |
| ***Source to WG:*** | ZTE, Keysight |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-07-26 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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). It is not clear if the gNB/ng-eNB fails to verifiy the ResumeMAC-I/shortResumeMAC-I. |
|  |  |
| ***Summary of change:*** | Clarify if the gNB/ng-eNB fails to verifiy the ResumeMAC-I/shortResumeMAC-I. |
|  |  |
| ***Consequences if not approved:*** | uncompleted specification. |
|  |  |
| ***Clauses affected:*** | 6.8.2.1.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS33.511 ... CR 0031...  |
| ***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 \*\*\*

##### 6.8.2.1.3 State transition from RRC\_INACTIVE to RRC\_CONNECTED to a new gNB/ng-eNB

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 I-RNTI (short or full I-RNTI) is used for context identification and its value shall be the same as the I-RNTI that the UE had received from the source gNB/ng-eNB in the RRCRelease with *suspendConfig* message. The ResumeMAC-I/shortResumeMAC-I is a 16-bit message authentication token, the UE shall calculate it using the integrity algorithm (NIA or EIA) in the stored AS security context, which was negotiated between the UE and the source gNB/ng-eNB and the current KRRCint with the following inputs:

- KEY : it shall be set to current KRRCint;

- BEARER : all its bits shall be set to 1.

- DIRECTION : its bit shall be set to 1;

- COUNT : all its bits shall be set to 1;

- MESSAGE : it shall be set to VarResumeMAC-Input/VarShortInactiveMAC-Input as defined in TS 38.331 [22] for gNB and in TS 36.331 [69] for ng-eNB with following inputs:

 *source PCI, target Cell-ID, source C-RNTI*.

For protection of all RRC messages except RRCReject message following the sent RRCResumeRequest message, the UE shall derive a KNG-RAN\* using the target PCI, target ARFCN-DL/EARFCN-DL and the KgNB/NH based on either a horizontal key derivation or a vertical key derivation as defined in clause 6.9.2.1.1 and Annex A.11/Annex A.12. The UE shall further derive KRRCint, KRRCenc, KUPenc (optionally), and KUPint (optionally) from the newly derived KNG-RAN\*.

When the target gNB/ng-eNB receives the RRCResumeRequest message from the UE, the target gNB/ng-eNB extracts the I-RNTI from the RRCResumeRequest message. The target gNB/ng-eNB contacts the source gNB/ng-eNB based on the information in the I-RNTI by sending an Xn-AP Retrieve UE Context Request message with the following included: I-RNTI, the ResumeMAC-I/shortResumeMAC-I and target Cell-ID, in order to allow the source gNB/ng-eNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.

The source gNB/ng-eNB retrieves the stored UE context including the UE 5G AS security context from its database using the I-RNTI. 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). If the verification of the ResumeMAC-I/shortResumeMAC-I is successful, then the source gNB/ng-eNB calculates KNG-RAN\* using the target cell PCI, target ARFCN-DL/EARFCN-DL and the KgNB/NH in the current UE 5G AS security context based on either a horizontal key derivation or a vertical key derivation according to whether the source gNB/ng-eNB has an unused pair of {NCC, NH} as described in Annex A.11/Annex A.12.If the verification of the ResumeMAC-I/shortResumeMAC-I has failed, then the RRC integrity mechanisms are applicable as specified by clause 6.5.1 of this document. The source gNB/ng-eNB can obtain the target PCI and target ARFCN-DL/EARFCN-DL from a cell configuration database by means of the target Cell-ID which was received from the target gNB/ng-eNB. Then the source gNB/ng-eNB shall respond with an Xn-AP Retrieve UE Context Response message to the target gNB/ng-eNB including the UE context that contains the UE 5G AS security context. The UE 5G AS security context sent to the target gNB/ng-eNB shall include the newly derived KNG-RAN\*, the NCC associated to the KNG-RAN\*, the UE 5G security capabilities, UP security policy, the UP security activation status with the corresponding PDU session ID(s), and the ciphering and integrity algorithms used by the UE with the source cell.

The target gNB/ng-eNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target gNB/ng-eNB does not support the ciphering and integrity algorithms used in the last source cell or if the target gNB/ng-eNB prefers to use different algorithms than the source gNB/ng-eNB, then the target gNB/ng-eNB shall send an RRC Setup/RRCSetup message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC\_IDLE (i.e., a fallback procedure).

If the target gNB/ng-eNB supports the ciphering and integrity algorithms used with the last source cell and these algorithms are the chosen algorithms by the target gNB/ng-eNB, the target gNB/ng-eNB shall derive new AS keys (RRC integrity key, RRC encryption key and UP keys) using the algorithms the UE used with the source cell and the received KNG-RAN\*. The target gNB/ng-eNB shall reset all PDCP COUNTs to 0 and activate the new keys in PDCP layer. The target gNB/ng-eNB shall respond to the UE with an RRC Resume message on SRB1 which is integrity protected and ciphered in PDCP layer using the new RRC keys.

If the UP security activation status can be supported in the target gNB/ng-eNB, the target gNB/ng-eNB shall use the UP security activations that the UE used at the last source cell. Otherwise, the target gNB/ng-eNB shall respond with an RRC Setup message to establish a new RRC connection with the UE.

When the UE receives the RRCResume message, the UE shall decrypt the message using the KRRCenc that was derived based on the newly derived KNG-RAN\*. The UE shall also verify the <RRC Connection Resume> message by verifying the PDCP MAC-I using the KRRCint that was derived from the newly derived KNG-RAN\* If verification of the RRCResume message is successful, the UE shall delete the current KRRCint key and the UE shall save the KRRCint, KRRCenc, KUPenc (optionally), and KUPint (optionally) from the newly derived KNG-RAN\* as part of the UE current AS security context. In this case, the UE shall send the RRCResumeComplete message both integrity protected and ciphered to the target gNB/ng-eNB on SRB1 using the current KRRCint and KRRCenc. The UE shall use the UP security activations that were used before tansition to the RRC Inactive.

If the UE receives RRCReject message from the target gNB/ng-eNB in response to the UE <RRC Resume Request> message, the UE shall delete newly derived AS keys used for connection resumption attempt, including newly derived KNG-RAN\*, newly derivedRRC integrity key, RRC encryption key and UP keys, and keep the current KRRCint and the KgNB/NH in its current AS context.

Security is fully resumed on UE side after reception and processing of RRCResume message. The UE can receive data on DRB(s) after having received and processed RRC connection resume message. UL data on DRB(s) can be sent after RRCResumeComplete message has been successfully sent.

After a successful transition from RRC\_INACTIVE to RRC\_CONNECTED the target gNB/ng-eNB shall perform Path Switch procedure with the AMF. The AMF shall verify the UE security capability as described in the clause 6.7.3.1, and the SMF shall veirfy the UE security policy as described in the clause 6.6.1.

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