**3GPP TSG-SA3 Meeting #108-e *draft\_S3-222021-r5***

**Online, , 22nd Aug 2022 - 26th Aug 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **-** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for SERP: draftCR to TS 33.501 on the Protection of the RRC Resume Request message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SERP | | | | |  | ***Date:*** | | | 2022-08-15 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **C** |  | | | | | ***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 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:*** | | It was agreed in SA3 to integrity protect the RRC Resume Request message as per SP-220538. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The procedure for the integrity protection of the RRC Resume Request message and the details of the message protection are specified.  The changes include the following:  - Support and usage requirements  - Changes to the calculation of the ResumeMAC-I/shortResumeMAC-I by the UE and source gNB/ng-eNB.  - Changes to the RRC Release procedure, system information, and UE capabilities to allow the different network entities to determine how to calculate the ResumeMAC-I/shortResumeMAC-I for message inclusion or verification purposes. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Insecure RRC Resume procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.3, 5.3.3, 5.4 , 6.8.2.1.1, 6.8.2.1.2, 6.8.2.1.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

**\*\*\* START OF CHANGES \*\*\***

5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

The UE shall support the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message.

**\*\*\* NEXT CHANGE \*\*\***

5.3.3 User data and signalling data integrity

The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

The gNB shall activate integrity protection of user data based on the security policy sent by the SMF.

The gNB shall support integrity protection and replay protection of RRC-signalling.

The gNB shall support the following integrity protection algorithms:

- NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The gNB may support the following integrity protection algorithm:

- 128-NIA3 as defined in Annex D of the present document.

Integrity protection of the user data between the UE and the gNB is optional to use, and shall not use NIA0.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB. NIA0 will add an unnecessary overhead of 32-bits MAC with no security benefits.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

NIA0 shall be disabled in gNB in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

The gNB shall support the calculation of the ResumeMAC-I using the whole RRCResumeRequest message.

**\*\*\* NEXT CHANGE \*\*\***

5.4 Requirements on the ng-eNB

The security requirements for ng-eNB are as specified for eNB in TS 33.401 [10] with the following additional requirement:

- ng-eNB shall support the use of integrity protection with the UE over the Uu interface.

- ng-eNB shall support the calculation of the shortResumeMAC-I using the whole RRC ResumeRequestmessage.

**\*\*\* NEXT CHANGE \*\*\***

6.8.2 Security handling at RRC state transitions

6.8.2.1 Security handling at transitions between RRC\_INACTIVE and RRC\_CONNECTED states

6.8.2.1.1 General

In 5G, the RRC\_INACTIVE state allows gNB/ng-eNB to suspend the UE's RRC connection while the gNB/ng-eNB and the UE continue to maintain the UE 5G AS security context. The UE RRC connection can be resumed at a later time by allowing the UE to transition into RRC\_\_CONNECTED state. The UE may transition from RRC\_INACTIVE state to RRC\_CONNECTED state to the same last serving gNB/ng-eNB which sent the UE into RRC\_INACTIVE state or to a different gNB/ng-eNB. While the UE is in RRC\_INACTIVE state, the UE and last serving gNB/ng-eNB store the UE 5G AS security context which can be reactivated when the UE transitions from RRC\_INACTIVE to RRC\_CONNECTED. The gNB/ng-eNB and the UE shall behave as defined in following sub-clauses. The ng-eNB connected to 5GC shall also support the same security handling at RRC state transitions.

With the exception of backward compatibility when connecting with legacy entities, the UE and gNB/ng-eNB shall use the ResumeMAC-I/shortResumeMAC-I calculated using the whole RRCResumeRequest message. The gNB/ng-eNB shall broadcast an indication in its System Information that UEs connecting to it shall use the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message. The UE shall indicate to the network in the UE's capabilities that the UE supports the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message.

6.8.2.1.2 State transition from RRC\_CONNECTED to RRC\_INACTIVE

The gNB/ng-eNB shall send to the UE an RRCRelease with *suspendConfig* message that is ciphered and integrity protected in PDCP layer using a current AS security context. The gNB/ng-eNB shall include a fresh I-RNTI, an NCC, and an indication to use the ResumeMAC-I/shortResumeMAC-I calculated using the whole RRCResumeRequest message in that RRCRelease with *suspendConfig* message. The I-RNTI is used for context identification, and the UE ID part of the I-RNTI assigned by the gNB/ng-eNB shall be different in consecutive suspends of the same UE. This is to avoid tracking of UEs based on the I-RNTI. If the gNB/ng-eNB has a fresh and unused pair of {NCC, NH}, the gNB/ng-eNB shall include the NCC in the RRCRelease with *suspendConfig* message. Otherwise, the gNB/ng-eNB shall include the same NCC associated with the current KgNB in the RRCRelease with *suspendConfig* message. The NCC is used for AS security.

The gNB/ng-eNB shall delete the current AS keys KRRCenc, KUPenc (if available), and KUPint (if available) after sending the RRCRelease with *suspendConfig* message to the UE, but shall keep the current AS key KRRCint. If the sent NCC value is fresh and belongs to an unused pair of {NCC, NH}, the gNB/ng-eNB shall save the pair of {NCC, NH} in the current UE AS security context and shall delete the current AS key KgNB. If the sent NCC value is equal to the NCC value associated with the current KgNB, the gNB/ng-eNB shall keep the current AS key KgNB and NCC. The gNB/ng-eNB shall store the sent I‑RNTI together with the current UE context including the remainder of the AS security context.

Upon receiving the RRC Release with *suspendConfig* message from the gNB/ng-eNB, the UE shall verify that the integrity of the received RRCRelease with *suspendConfig* message is correct by checking the PDCP MAC-I. If this verification is successful, then the UE shall take the received NCC value and save it as stored NCC with the current UE context. The UE shall delete the current AS keys KRRCenc, KUPenc (if available), and KUPint (if available), but keep the current AS key KRRCint key. If the stored NCC value is different from the NCC value associated with the current KgNB, the UE shall delete the current AS key KgNB. If the stored NCC is equal to the NCC value associated with the current KgNB, the UE shall keep the current AS key KgNB. The UE shall store the received I-RNTI and the received indication to use the ResumeMAC-I/shortResumeMAC-I calculated using the whole RRCResumeRequest message together with the current UE context including the remainder of the AS security context, for the next state transition.

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

As defined in the clause 6.8.2.1.1, the target gNB/ng-eNB broadcasts an indication in its System Information that the UEs connecting to it shall use the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message. Using this indication, the UE shall determine that the target gNB/ng-eNB supports the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message.

Further, using the stored indication the UE had received from the source gNB/ng-eNB to use the ResumeMAC-I/shortResumeMAC-I calculated using the whole RRCResumeRequest message, the UE shall determine that the source gNB/ng-eNB supports the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message.

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 :

- if the UE determines that both the source gNB/ng-eNB and the target gNB/ng-eNB support the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message, the MESSAGE input shall be set to Var2ResumeMAC-Input/Var2ShortResumeMAC-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, whole* RRCResumeRequest *message with the ResumeMAC-I/shortResumeMAC-I IE set to all zeros or the whole* RRCResumeRequest *message without the ResumeMAC-I/shortResumeMAC-I IE*.

Editor's Note: Whether to perform the calculation of ResumeMAC-Input/shortResumeMAC-I with the whole RRCResumeRequest message with the ResumeMAC-Input/shortResumeMAC-I set to all zeros or the whole RRCResumeRequest message without the ResumeMAC-Input/shortResumeMAC-I IE is to be decided by the RAN groups.

Editor's Note: The Var2ResumeMAC-Input/Var2ShortResumeMAC-Input are to be specified from RAN groups

- if the UE determines that either the source gNB/ng-eNB or the target gNB/ng-eNB does not support the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message, the MESSAGE input 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. If the target gNB/ng-eNB supports the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message, the target gNB/ng-eNB shall additionally include the remaining IEs in the RRCResumeRequest message (e.g. resume cause, and spare IE) in the Retrieve UE Context Request message.

Editor's Note: Whether to include the whole RRCResumeRequest message in the Xn-AP Retrieve UE Context Request message is to be decided by RAN3. The paragraph may be updated based on the decision in RAN3.

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 with the following differences). If the source gNB/ng-eNB determines that both the UE and the target gNB/ng-eNB support the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message, the MESSAGE input shall be set to Var2ResumeMAC-Input/Var2ShortResumeMAC-Input. Otherwise, if the source gNB/ng-eNB determines that either the UE or the target gNB/ng-eNB does not support the calculation of the ResumeMAC-I/shortResumeMAC-I using the whole RRCResumeRequest message, the MESSAGE input shall be set to VarResumeMAC-Input/VarShortInactiveMAC-Input.

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. 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 target gNB/ng-eNB rejects the RRC Resume Request by sending RRCReject message, then it shall indicate the reject cause (e.g. wrong version of ResumeMAC-I) and the original “resumecause” in the Resume Reject message to make UE to verify. 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.

Editor's Note: The RRC Reject handling remains to be clarified according to Solution #17, TR 33.809.

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 \*\*\***