**3GPP TSG-RAN WG2 Meeting #117eR2-22xxxx**

**e-Meeting, 21st Feb – 3rd March 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **38.331** | **CR** | **2900** | **rev** | **-**  | **Current version:** | **16.7.0** |  |
|  |
| *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 |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Correction of NCC storage during re-establishment and Resume |
|  |  |
| ***Source to WG:*** | Intel Corporation |
| ***Source to TSG:*** | RAN2 |
|  |  |
| ***Work item code:*** | NR\_newRAT-Core |  | ***Date:*** | 2022-02-14 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-16 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The current specification text related to the storage and usage of NCC during Resume procedure is not consistent with the corresponding description in the SA3 specifications (33.501) and hence is incorrect. Specifically:1. During the re-establishment procedure, received NCC is stored before the keys are generated.
2. The storage of NCC during resume procedure is incorrect. The value received in RRC release should be stored in UE Inactive context for subsequent use. And the value of NCC used for key generation should be stored after receipt of the Resume message and also on receipt of RRC release in response to ResumeRequest. As there are two NCC values stored, one in the UE AS context and one in UE Inactive context, it is not clear which NCC is used for key derivation during ResumeRequest.

The issues are discussed in Tdoc R2-2202637 |
|  |  |
| ***Summary of change:*** | The description of the handling of NCC is aligned with the corresponding description in 33.501, as follows : 1. The storage of NCC is moved to after key generation in the procedural text for re-establishment
2. nextHopChainingCount received in RRC Release message is stored in UE Inactive context. The value of nextHopChainingCount used for the current keys is stored on receipt of Resume message and also on receipt of RRC Release in response to a ResumeRequest. It is clarified that the value of nextHopChainingCount received in RRCRelease message and stored in UE Inactive context is used for key derivation during ResumeRequest procedure.

Impact Analysis:The CR only impacts the UE. There are no interoperability issues foreseen as the CR is aligning the description in the RRC specs with that in the 33.501 (which was previously anyway used as reference for the handling of NCC).  |
|  |  |
| ***Consequences if not approved:*** | Handing of NCC in the RRC spec is not aligned with the description in 33.501 and the gaps in the protocol handling of NCC will remain.  |
|  |  |
| ***Clauses affected:*** | 5.3.7.5, 5.3.8.3, 5.3.13.3, 5.3.13.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **Y** |  |  Other core specifications  | TS38.331 CR2899 |
| ***affected:*** |  |  |  Test specifications |  |
| ***(show related CRs)*** |  |  |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

#### 5.3.7.5 Reception of the *RRCReestablishment* by the UE

The UE shall:

1> stop timer T301;

1> consider the current cell to be the PCell;

1> update the KgNB key based on the current KgNB key or the NH*,* using the received *nextHopChainingCount* value, as specified in TS 33.501 [11];

1> store the *nextHopChainingCount* value indicated in the *RRCReestablishment* message;

1> derive the KRRCenc and KUPenc keys associated with the previously configured *cipheringAlgorithm,* as specified in TS 33.501 [11];

1> derive the KRRCint and KUPint keys associated with the previously configured *integrityProtAlgorithm,* as specified in TS 33.501 [11].

1> request lower layers to verify the integrity protection of the *RRCReestablishment* message, using the previously configured algorithm and the KRRCint key;

1> if the integrity protection check of the *RRCReestablishment* message fails:

2> perform the actions upon going to RRC\_IDLE as specified in 5.3.11, with release cause 'RRC connection failure', upon which the procedure ends;

1> configure lower layers to resume integrity protection for SRB1 using the previously configured algorithm and the KRRCint key immediately, i.e., integrity protection shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

1> configure lower layers to resume ciphering for SRB1 using the previously configured algorithm and, the KRRCenc key immediately, i.e., ciphering shall be applied to all subsequent messages received and sent by the UE, including the message used to indicate the successful completion of the procedure;

1> release the measurement gap configuration indicated by the *measGapConfig*, if configured;

1> set the content of *RRCReestablishmentComplete* message as follows:

2> if the UE has logged measurements available for NR and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport*:

3> include the *logMeasAvailable* in the *RRCReestablishmentComplete* message;

3> if Bluetooth measurement results are included in the logged measurements the UE has available for NR:

4> include the *logMeasAvailableBT* in the *RRCReestablishmentComplete* message;

3> if WLAN measurement results are included in the logged measurements the UE has available for NR:

4> include the *logMeasAvailableWLAN* in the *RRCReestablishmentComplete* message;

2> if the UE has connection establishment failure or connection resume failure information available in *VarConnEstFailReport* and if the RPLMN is equal to *plmn-Identity* stored in *VarConnEstFailReport*:

3> include *connEstFailInfoAvailable* in the *RRCReestablishmentComplete* message;

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report*; or

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* of TS 36.331 [10] and if the UE is capable of cross-RAT RLF reporting and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report* of TS 36.331 [10]:

3> include *rlf-InfoAvailable* in the *RRCReestablishmentComplete* message;

1> submit the *RRCReestablishmentComplete* message to lower layers for transmission;

1> the procedure ends.

|  |
| --- |
| \*\*\*\*\* Next Change \*\*\*\*\* |

#### 5.3.8.3 Reception of the *RRCRelease* by the UE

The UE shall:

1> delay the following actions defined in this sub-clause 60 ms from the moment the *RRCRelease* message was received or optionally when lower layers indicate that the receipt of the *RRCRelease* message has been successfully acknowledged, whichever is earlier;

1> stop timer T380, if running;

1> stop timer T320, if running;

1> if timer T316 is running;

2> stop timer T316;

2> clear the information included in *VarRLF-Report,* if any;

1> stop timer T350, if running;

1> if theAS security is not activated:

2> ignore any field included in *RRCRelease* message except *waitTime*;

2> perform the actions upon going to RRC\_IDLE as specified in 5.3.11 with the release cause 'other' upon which the procedure ends;

1> if the *RRCRelease* message includes *redirectedCarrierInfo* indicating redirection to *eutra*:

2> if *cnType* is included:

3> after the cell selection, indicate the available CN Type(s) and the received *cnType* to upper layers;

NOTE 1: Handling the case if the E-UTRA cell selected after the redirection does not support the core network type specified by the *cnType,* is up to UE implementation.

2> if *voiceFallbackIndication* is included:

3> consider the RRC connection release was for EPS fallback for IMS voice (see TS 23.502 [43]);

1> if the *RRCRelease* message includes the *cellReselectionPriorities*:

2> store the cell reselection priority information provided by the *cellReselectionPriorities*;

2> if the *t320* is included:

3> start timer T320, with the timer value set according to the value of *t320*;

1> else:

2> apply the cell reselection priority information broadcast in the system information;

1> if *deprioritisationReq* is included and the UE supports RRC connection release with deprioritisation:

2> start or restart timer T325 with the timer value set to the *deprioritisationTimer* signalled;

2> store the *deprioritisationReq* until T325 expiry;

NOTE 1a: The UE stores the deprioritisation request irrespective of any cell reselection absolute priority assignments (by dedicated or common signalling) and regardless of RRC connections in NR or other RATs unless specified otherwise.

1> if the *RRCRelease* includes the *measIdleConfig*:

2> if T331 is running:

3> stop timer T331;

3> perform the actions as specified in 5.7.8.3;

2> if the *measIdleConfig* is set to *setup*:

3> store the received *measIdleDuration* in *VarMeasIdleConfig*;

3> start timer T331 with the value set to *measIdleDuration*;

3> if the *measIdleConfig* contains *measIdleCarrierListNR*:

4> store the received *measIdleCarrierListNR* in *VarMeasIdleConfig*;

3> if the *measIdleConfig* contains *measIdleCarrierListEUTRA*:

4> store the received *measIdleCarrierListEUTRA* in *VarMeasIdleConfig*;

3> if the *measIdleConfig* contains *validityAreaList*:

4> store the received *validityAreaList* in *VarMeasIdleConfig*;

1> if the *RRCRelease* includes *suspendConfig*:

2> apply the received *suspendConfig* except the received *nextHopChainingCount*;

2> remove all the entries within *VarConditionalReconfig*, if any;

2> for each *measId*, if the associated *reportConfig* has a *reportType* set to *condTriggerConfig*:

3> for the associated *reportConfigId*:

4> remove the entry with the matching *reportConfigId* from the *reportConfigList* within the *VarMeasConfig*;

3> if the associated *measObjectId* is only associated to a *reportConfig* with *reportType* set to *condTriggerConfig*:

4> remove the entry with the matching *measObjectId* from the *measObjectList* within the *VarMeasConfig*;

3> remove the entry with the matching *measId* from the *measIdList* within the *VarMeasConfig*;

2> reset MAC and release the default MAC Cell Group configuration, if any;

2> re-establish RLC entities for SRB1;

2> if the *RRCRelease* message with *suspendConfig* was received in response to an *RRCResumeRequest* or an *RRCResumeRequest1*:

3> stop the timer T319 if running;

3> in the stored UE Inactive AS context:

4> replace the KgNB and KRRCint keys with the current KgNB and KRRCint keys;

4> replace the *nextHopChainingCount* with the value received in the *RRCRelease* message*;*

4> replace the C-RNTI with the C-RNTI used in the cell (see TS 38.321 [3]) the UE has received the *RRCRelease* message;

4> replace the *cellIdentity* with the *cellIdentity* of the cell the UE has received the *RRCRelease* message;

4> replace the physical cell identitywith the physical cell identity of the cell the UE has received the *RRCRelease* message;

 3> replace the *nextHopChainingCount* corresponding to the current KgNB;

2> else:

3> store in the UE Inactive AS Context the *nextHopChainingCount* received in the *RRCRelease* message*,* the current KgNB and KRRCint keys, the ROHC state, the stored QoS flow to DRB mapping rules, the C-RNTI used in the source PCell, the *cellIdentity* and the physical cell identity of the source PCell, the *spCellConfigCommon* within *ReconfigurationWithSync* of the NR PSCell (if configured) and all other parameters configured except for:

- parameters within *ReconfigurationWithSync* of the PCell;

- parameters within *ReconfigurationWithSync* of the NR PSCell, if configured;

- parameters within *MobilityControlInfoSCG* of the E-UTRA PSCell, if configured;

- *servingCellConfigCommonSIB*;

NOTE 2: NR sidelink communication related configurations and logged measurement configuration are not stored as UE Inactive AS Context, when UE enters RRC\_INACTIVE.

2> suspend all SRB(s) and DRB(s), except SRB0;

2> indicate PDCP suspend to lower layers of all DRBs;

2> if the *t380* is included:

3> start timer T380, with the timer value set to *t380*;

2> if the *RRCRelease* message is including the *waitTime*:

3> start timer T302 with the value set to the *waitTime*;

3> inform upper layers that access barring is applicable for all access categories except categories '0' and '2';

2> if T390 is running:

3> stop timer T390 for all access categories;

3> perform the actions as specified in 5.3.14.4;

2> indicate the suspension of the RRC connection to upper layers;

2> enter RRC\_INACTIVE and perform cell selection as specified in TS 38.304 [20];

1> else

2> perform the actions upon going to RRC\_IDLE as specified in 5.3.11, with the release cause 'other'.

|  |
| --- |
| \*\*\*\*\* Next Change \*\*\*\*\* |

#### 5.3.13.3 Actions related to transmission of *RRCResumeRequest* or *RRCResumeRequest1* message

The UE shall set the contents of *RRCResumeRequest* or *RRCResumeRequest1* message as follows:

1> if field *useFullResumeID* is signalled in *SIB1*:

2> select *RRCResumeRequest1* as the message to use;

2> set the *resumeIdentity* to the stored *fullI-RNTI* value;

1> else:

2> select *RRCResumeRequest* as the message to use;

2> set the *resumeIdentity* to the stored *shortI-RNTI* value;

1> restore the RRC configuration, RoHC state, the stored QoS flow to DRB mapping rules and the KgNB and KRRCint keys from the stored UE Inactive AS context except for the following:

- masterCellGroup;

- mrdc-SecondaryCellGroup, if stored; and

- pdcp-Config;

1> set the *resumeMAC-I* to the 16 least significant bits of the MAC-I calculated:

2> over the ASN.1 encoded as per clause 8 (i.e., a multiple of 8 bits) *VarResumeMAC-Input*;

2> with the KRRCint key in the UE Inactive AS Context and the previously configured integrity protection algorithm; and

2> with all input bits for COUNT, BEARER and DIRECTION set to binary ones;

1> derive the KgNB key based on the current KgNB key or the NH, using the *nextHopChainingCount* value received in the previous *RRCRelease* message and stored in the UE Inactive AS Context, as specified in TS 33.501 [11];

1> derive the KRRCenc key, the KRRCint key, the KUPint key and the KUPenc key;

1> configure lower layers to apply integrity protection for all radio bearers except SRB0 using the configured algorithm and the KRRCint key and KUPint key derived in this subclause immediately, i.e., integrity protection shall be applied to all subsequent messages received and sent by the UE;

NOTE 1: Only DRBs with previously configured UP integrity protection shall resume integrity protection.

1> configure lower layers to apply ciphering for all radio bearers except SRB0 and to apply the configured ciphering algorithm, the KRRCenc key and the KUPenc key derived in this subclause, i.e. the ciphering configuration shall be applied to all subsequent messages received and sent by the UE;

1> re-establish PDCP entities for SRB1;

1> resume SRB1;

1> submit the selected message *RRCResumeRequest* or *RRCResumeRequest1* for transmission to lower layers.

NOTE 2: Only DRBs with previously configured UP ciphering shall resume ciphering.

If lower layers indicate an integrity check failure while T319 is running, perform actions specified in 5.3.13.5.

The UE shall continue cell re-selection related measurements as well as cell re-selection evaluation. If the conditions for cell re-selection are fulfilled, the UE shall perform cell re-selection as specified in 5.3.13.6.

#### 5.3.13.4 Reception of the *RRCResume* by the UE

The UE shall:

1> stop timer T319;

1> stop timer T380, if running;

1> if T331 is running:

2> stop timer T331;

2> perform the actions as specified in 5.7.8.3;

1> if the *RRCResume* includes the *fullConfig*:

2> perform the full configuration procedure as specified in 5.3.5.11;

1> else:

2> if the *RRCResume* does not include the *restoreMCG-SCells*:

3> release the MCG SCell(s) from the UE Inactive AS context, if stored;

2> if the *RRCResume* does not include the *restoreSCG*:

3> release the MR-DC related configurations (i.e., as specified in 5.3.5.10) from the UE Inactive AS context, if stored;

2> restore the *masterCellGroup, mrdc-SecondaryCellGroup*, if stored, and *pdcp-Config* from the UE Inactive AS context;

2> configure lower layers to consider the restored MCG and SCG SCell(s) (if any) to be in deactivated state;

1> discard the UE Inactive AS context;

1> store the used *nextHopChainingCount* value associated to the current KgNB;

1> release the *suspendConfig* except the *ran-NotificationAreaInfo*;

1> if the *RRCResume* includes the *masterCellGroup*:

2> perform the cell group configuration for the received *masterCellGroup* according to 5.3.5.5;

1> if the *RRCResume* includes the *mrdc-SecondaryCellGroup:*

2> if the received *mrdc-SecondaryCellGroup* is set to *nr-SCG*:

3> perform the RRC reconfiguration according to 5.3.5.3 for the *RRCReconfiguration* message included in *nr-SCG*;

2> if the received *mrdc-SecondaryCellGroup* is set to *eutra-SCG*:

3> perform the RRC connection reconfiguration as specified in TS 36.331 [10], clause 5.3.5.3 for the *RRCConnectionReconfiguration* message included in *eutra-SCG*;

1> if the *RRCResume* includes the *radioBearerConfig*:

2> perform the radio bearer configuration according to 5.3.5.6;

1> if the *RRCResume* message includes the *sk-Counter*:

2> perform security key update procedure as specified in 5.3.5.7;

1> if the *RRCResume* message includes the *radioBearerConfig2*:

2> perform the radio bearer configuration according to 5.3.5.6;

1> if the *RRCResume* message includes the *needForGapsConfigNR*:

2> if *needForGapsConfigNR* is set to *setup*:

3> consider itself to be configured to provide the measurement gap requirement information of NR target bands;

2> else:

3> consider itself not to be configured to provide the measurement gap requirement information of NR target bands;

1> resume SRB2, SRB3 (if configured), and all DRBs;

1> if stored, discard the cell reselection priority information provided by the *cellReselectionPriorities* or inherited from another RAT;

1> stop timer T320, if running;

1> if the *RRCResume* message includes the *measConfig*:

2> perform the measurement configuration procedure as specified in 5.5.2;

1> resume measurements if suspended;

1> if T390 is running:

2> stop timer T390 for all access categories;

2> perform the actions as specified in 5.3.14.4;

1> if T302 is running:

2> stop timer T302;

2> perform the actions as specified in 5.3.14.4;

1> enter RRC\_CONNECTED;

1> indicate to upper layers that the suspended RRC connection has been resumed;

1> stop the cell re-selection procedure;

1> consider the current cell to be the PCell;

1> set the content of the of *RRCResumeComplete* message as follows:

2> if the upper layer provides NAS PDU, set the *dedicatedNAS-Message* to include the information received from upper layers;

2> if upper layers provides a PLMN and UE is either allowed or instructed to access the PLMN via a cell for which at least one CAG ID is broadcast:

3> set the *selectedPLMN-Identity* from the *npn-IdentityInfoList*;

2> else:

3> set the *selectedPLMN-Identity* to the PLMN selected by upper layers from the *plmn-IdentityInfoList*;

2> if the *masterCellGroup* contains the *reportUplinkTxDirectCurrent*:

3> include the *uplinkTxDirectCurrentList* for each MCG serving cell with UL;

3> include *uplinkDirectCurrentBWP-SUL* for each MCG serving cell configured with SUL carrier, if any, within the *uplinkTxDirectCurrentList*;

2> if the *masterCellGroup* contains the *reportUplinkTxDirectCurrentTwoCarrier*:

3> include in the *uplinkTxDirectCurrentTwoCarrierList* the list of uplink Tx DC locations for the configured uplink carrier aggregation in the MCG;

2> if the UE has idle/inactive measurement information concerning cells other than the PCell available in *VarMeasIdleReport*:

3> if the *idleModeMeasurementReq* is included in the *RRCResume* message:

4> set the *measResultIdleEUTRA* in the *RRCResumeComplete* message to the value of *measReportIdleEUTRA* in the *VarMeasIdleReport,* if available;

4> set the *measResultIdleNR* in the *RRCResumeComplete* message to the value of *measReportIdleNR* in the *VarMeasIdleReport*, if available;

4> discard the *VarMeasIdleReport* upon successful delivery of the *RRCResumeComplete* message is confirmed by lower layers;

3> else:

4> if the SIB1 contains *idleModeMeasurementsNR* and the UE has NR idle/inactive measurement information concerning cells other than the PCell available in *VarMeasIdleReport*; or

4> if the SIB1 contains *idleModeMeasurementsEUTRA* and the UE has E-UTRA idle/inactive measurement information available in *VarMeasIdleReport*:

5> include the *idleMeasAvailable*;

2> if the *RRCResume* message includes *mrdc-SecondaryCellGroup* set to *eutra-SCG*:

3> include in the *eutra-SCG-Response* the E-UTRA *RRCConnectionReconfigurationComplete* message in accordance with TS 36.331 [10] clause 5.3.5.3;

2> if the *RRCResume* message includes *mrdc-SecondaryCellGroup* set to *nr-SCG*:

3> include in the *nr-SCG-Response* the SCG *RRCReconfigurationComplete* message;

2> if the UE has logged measurements available for NR and if the RPLMN is included in *plmn-IdentityList* stored in *VarLogMeasReport*:

3> include the *logMeasAvailable* in the *RRCResumeComplete* message*;*

3> if Bluetooth measurement results are included in the logged measurements the UE has available for NR:

4> include the *logMeasAvailableBT* in the *RRCResumeComplete* message;

3> if WLAN measurement results are included in the logged measurements the UE has available for NR:

4> include the *logMeasAvailableWLAN* in the *RRCResumeComplete* message;

2> if the UE has connection establishment failure or connection resume failure information available in *VarConnEstFailReport* and if the RPLMN is equal to *plmn-Identity* stored in *VarConnEstFailReport*:

3> include *connEstFailInfoAvailable* in the *RRCResumeComplete* message;

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report*; or

2> if the UE has radio link failure or handover failure information available in *VarRLF-Report* of TS 36.331 [10] and if the UE is capable of cross-RAT RLF reporting and if the RPLMN is included in *plmn-IdentityList* stored in *VarRLF-Report* of TS 36.331 [10]:

3> include *rlf-InfoAvailable* in the *RRCResumeComplete* message;

2> if the UE supports storage of mobility history information and the UE has mobility history information available in *VarMobilityHistoryReport*:

3> include the *mobilityHistoryAvail* in the *RRCResumeComplete* message;

2> if *speedStateReselectionPars* is configured in the *SIB2*:

3> include the *mobilityState* in the *RRCResumeComplete* message and set it to the mobility state (as specified in TS 38.304 [20]) of the UE just prior to entering RRC\_CONNECTED state;

2> if the UE is configured to provide the measurement gap requirement information of NR target bands:

3> include the *NeedForGapsInfoNR* and set the contents as follows:

4> include *intraFreq-needForGap* and set the gap requirement information of intra-frequency measurement for each NR serving cell;

4> if *requestedTargetBandFilterNR* is configured, for each supported NR band that is also included in *requestedTargetBandFilterNR*, include an entry in *interFreq-needForGap* and set the gap requirement information for that band; otherwise, include an entry in *interFreq-needForGap* and set the corresponding gap requirement information for each supported NR band;

1> submit the *RRCResumeComplete* message to lower layers for transmission;

1> the procedure ends.