**3GPP TSG-CT WG1 Meeting #131-eC1-21xxxx**

**E-meeting, 19-27 August 2021 (was C1-214305)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.301** | **CR** | **3526** | **rev** | **4** | **Current version:** | 17.3.0 |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | MME handling retransmission of TAU request during N26 inter-system change from N1 mode to S1 mode in idle mode | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2021-08-19 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | During field testing of N26 inter-system change from N1 mode to S1 mode in idle mode (see Figure 8.5.2-1 in TS 33.501) the following scenario was observed:   1. UE is redirected from 5G to 4G or UE reselects to 4G cell. 2. UE initiates the TAU procedure with NAS Uplink COUNT x for integrity protection computation. 3. After sending the embedded NAS message in the RRC message, UE experiences RLF and lower layer indicates transmission failure. However, LTE network has fully received the NAS message and forwards it to MME. 4. AMF verifies the integrity of the TAU request and performs KAMF to KASME' derivation using NAS Uplink COUNT x as described in TS 33.501 annex A.14.1 and includes the mapped EPS NAS security context in the Context Response message to the MME. 5. UE tries to re-transmit the TAU Request with identical content but with NAS Uplink COUNT to x + 1. 6. Steps #2 to #4 are repeated 7. MME follows either abnormal handling of case d) or e) defined in TS 24.301 subclause 5.5.3.2.7 which mandate MME to ignore the new identical content TAU request message and proceed with previous NAS message using security context derived in step #4 8. UE creates new mapped EPS NAS security context based upon latest NAS Uplink COUNT = x + 1 to be used to verify the integrity of TAU accept. 9. UE receives TAU accept but it does not pass integrity check because the UE is using NAS Uplink COUNT = x + 1 whereas the TAU accept was protected assuming NAS Uplink COUNT = x, so the TAU accept is ignored. 10. At expiry of T3450 timer (= 6 sec), MME keeps sending same TAU accept which is ignored by the UE. 11. After at least 5\*T3450= 30 sec, MME aborts the ongoing TAU procedure. 12. After two expiries of T3430 (=15 sec), UE sends TAU request which gets accepted by MME and and receives TAU accept which passes integrity check at UE side.   In order to avoid delaying UE receiving LTE service for at least 30 seconds, MME either run the authentication and activate new native EPS security context or if AMF is still having the old UE context, MME forwards it to source AMF for integrity check and providing latest mapped EPS security context.  Note that the option of UE sending 2nd TAU request using same NAS Uplink COUNT = x should not be adopted due to its security risk. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | For the case of receiving 2nd TAU request message with the same information elements after sending TAU accept or before sending TAU accept/reject, MME forwards the message to source AMF and if it passes the intergity check continue with new/ongoing procedure and protect any future NAS message to the UE using the latest mapped EPS security context. Alternative to forwarding 2nd TAU request to source AMF, MME can run authentication and activate new native EPS security context to be used to protect any future NAS message to the UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | During inter-system change from N1 mode to S1 mode in EMM-IDLE mode using N26 interface, UE might not be able to receive LTE service for at least 30 seconds because of security context mis-match between UE and MME. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.5.3.2.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Same as C1-213932 | | | | | | | | |

\*\*\*\*\* Next change \*\*\*\*\*

##### 5.5.3.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) If a lower layer failure occurs before the message TRACKING AREA UPDATE COMPLETE has been received from the UE and a GUTI has been assigned, the network shall abort the procedure, enter EMM-IDLE mode and shall consider both, the old and new GUTI as valid until the old GUTI can be considered as invalid by the network (see clause 5.4.1.4). During this period the network may use the identification procedure followed by a GUTI reallocation procedure if the old GUTI is used by the UE in a subsequent message.

The network may page with IMSI if paging with old and new S-TMSI fails. Paging with IMSI causes the UE to re-attach as described in clause 5.6.2.2.2.

b) Protocol error

If the TRACKING AREA UPDATE REQUEST message has been received with a protocol error, the network shall return a TRACKING AREA UPDATE REJECT message with one of the following EMM cause values:

#96: invalid mandatory information element error;

#99: information element non-existent or not implemented;

#100: conditional IE error; or

#111: protocol error, unspecified.

c) T3450 time-out

On the first expiry of the timer, the network shall retransmit the TRACKING AREA UPDATE ACCEPT message and shall reset and restart timer T3450. The retransmission is performed four times, i.e. on the fifth expiry of timer T3450, the tracking area updating procedure is aborted. Both, the old and the new GUTI shall be considered as valid until the old GUTI can be considered as invalid by the network (see clause 5.4.1.4). During this period the network acts as described for case a above.

d) TRACKING AREA UPDATE REQUEST received after the TRACKING AREA UPDATE ACCEPT message has been sent and before the TRACKING AREA UPDATE COMPLETE message is received

- If one or more of the information elements in the TRACKING AREA UPDATE REQUEST message differ from the ones received within the previous TRACKING AREA UPDATE REQUEST message, the previously initiated tracking area updating procedure shall be aborted if the TRACKING AREA UPDATE COMPLETE message has not been received and the new tracking area updating procedure shall be progressed; or

- If the information elements do not differ for cases other than inter-system change from N1 mode to S1 mode in EMM-IDLE mode with the UE operating in the single-registration mode, then the TRACKING AREA UPDATE ACCEPT message shall be resent and the timer T3450 shall be restarted if a TRACKING AREA UPDATE COMPLETE message is expected. If the information elements do not differ for the case of inter-system change from N1 mode to S1 mode in EMM-IDLE mode with the UE operating in the single-registration mode, the MME should forward the new TRACKING AREA UPDATE REQUEST message which contains the same information elements as the previous TRACKING AREA UPDATE REQUEST message to the source AMF to run the integrity check, obtain the latest mapped EPS security context (to be used to protect any future NAS message sent to the UE) and continue with the new tracking area updating procedure. In these cases, the retransmission counter related to T3450 is not incremented.

NOTE 1: Instead of forwarding the new TRACKING AREA UPDATE REQUEST message which contains the same information elements to the source AMF, the MME can decide to initiate an authentication procedure followed by a security mode control procedure to take the new partial native EPS security context into use and, if the new partial native EPS security context is taken into use successfully, then resend the same TRACKING AREA UPDATE ACCEPT message protected using this new EPS security context.

e) More than one TRACKING AREA UPDATE REQUEST received and no TRACKING AREA UPDATE ACCEPT or TRACKING AREA UPDATE REJECT message has been sent

- If one or more of the information elements in the TRACKING AREA UPDATE REQUEST message differs from the ones received within the previous TRACKING AREA UPDATE REQUEST message, the previously initiated tracking area updating procedure shall be aborted and the new tracking area updating procedure shall be progressed;

- if the information elements do not differ for cases other than inter-system change from N1 mode to S1 mode in EMM-IDLE mode with the UE operating in the single-registration mode, then the network shall continue with the previous tracking area updating procedure and shall not treat any further this TRACKING AREA UPDATE REQUEST message. If the information elements do not differ for the case of inter-system change from N1 mode to S1 mode in EMM-IDLE mode with the UE operating in the single-registration mode, the MME should forward the new TRACKING AREA UPDATE REQUEST message which contains the same information elements as the previous TRACKING AREA UPDATE REQUEST message to the source AMF to run the integrity check, obtain the latest mapped EPS security context (to be used to protect any future NAS message sent to the UE) and continue with the previous tracking area updating procedure.

NOTE 2: Instead of forwarding the new TRACKING AREA UPDATE REQUEST message which contains the same information elements to the source AMF, the MME can decide to initiate an authentication procedure followed by a security mode control procedure to take the new partial native EPS security context into use and, if the new partial native EPS security context is taken into use successfully, use this new EPS security context to protect any future NAS message sent to the UE.

f) Lower layers indication of non-delivered NAS PDU due to handover

If the TRACKING AREA UPDATE ACCEPT message or TRACKING AREA UPDATE REJECT message could not be delivered due to an intra MME handover and the TAI of the target cell and the TAI of the source cell are the same, then upon successful completion of the intra MME handover the MME shall retransmit the TRACKING AREA UPDATE ACCEPT message or TRACKING AREA UPDATE REJECT message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the TRACKING AREA UPDATE ACCEPT message or TRACKING AREA UPDATE REJECT message.

g) DETACH REQUEST message received before the TRACKING AREA UPDATE ACCEPT message is sent or before the TRACKING AREA UPDATE COMPLETE message (in case of GUTI and/or TMSI was allocated) is received.

Detach containing cause "switch off":

The network shall abort the signalling for the tracking area updating procedure towards the UE and shall progress the detach procedure as described in clause 5.5.2.2.

NOTE 3: Internally in the network, before processing the detach request, the MME can perform the necessary signalling procedures for the tracking area updating procedure before progressing the detach procedure.

Detach containing other causes than "switch off":

The network shall proceed with the tracking area updating procedure and shall progress the detach procedure after successful completion of the tracking area updating procedure.

h) If the TRACKING AREA UPDATE REQUEST message with EPS update type IE indicating "periodic updating" is received by the new MME which does not have the EMM context data related to the subscription, the new MME may send the TRACKING AREA UPDATE REJECT message with EMM cause value #10 "Implicitly detached"

\*\*\*\*\* End of changes \*\*\*\*\*