**3GPP TSG-CT WG1 Meeting #133-eC1-217118**

**E-meeting, 11-19 November 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.301** | **CR** | **3650** | **rev** | **-** | **Current version:** | **17.4.1** |  |
|  |
| *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:***  | Authentication failure when emergency bearer service is ongoing |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2021-11-04 |
|  |  |  |  |  |
| ***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 discussed in the discussion paper C1-214373, there is an ambiguity in the UE behavior in 5G and 4G as suggested by the RAN5 LS R5-213429. when the authentication failure happens during an emergency bearer service is ongoing, both the UE and the NW will continue with the emergency bearer service and release all the non-emergency EPS bearers. UE shall not consider the cell as barred. Both UE and the NW will consider itself as emergency registered. So in this situation, after the emergency EPS bearer is released, UE will have to do a de-registration, so that both UE and NW can move out of the emergency registered state.  |
|  |  |
| ***Summary of change:*** | Clarified the UE behavior on getting an authentication failure when a) an emergency bearer service is started or ongoing.b) No emergency bearer service is started or ongoing. Also the duplicated texts for cases #20, #21 and #26 are now grouped together to clarify the UE behavior when an emergerncy bearer service is ongoig or not. |
|  |  |
| ***Consequences if not approved:*** | Ambiguity in specification on how the UE should behave when an authentication failure happens during an emergency bearer service. |
|  |  |
| ***Clauses affected:*** | 5.4.1.2.4.5, 5.4.1.3.7 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \* \*

#####

#### 5.4.2.7 Abnormal cases

a) Lower layer failure:

 Upon detection of lower layer failure before the AUTHENTICATION RESPONSE message is received, the network shall abort the procedure.

b) Expiry of timer T3460:

 The network shall, on the first expiry of the timer T3460, retransmit the AUTHENTICATION REQUEST message and shall reset and start timer T3460. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3460, the network shall abort the authentication procedure and any ongoing EMM specific procedure and release the NAS signalling connection.

c) Authentication failure (EMM cause #20 "MAC failure"):

 The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #20 "MAC failure" according to clause 5.4.2.6, to the network and start timer T3418 (see example in figure 5.4.2.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3410, T3417, T3421 or T3430). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause #20 "MAC failure", the network may initiate the identification procedure described in clause 5.4.4. This is to allow the network to obtain the IMSI from the UE. The network may then check that the GUTI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the UE shall send the IDENTITY RESPONSE message.

NOTE 1: Upon receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause #20 "MAC failure", the network may also terminate the authentication procedure (see clause 5.4.2.5).

 If the GUTI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the UE. Upon receiving the new AUTHENTICATION REQUEST message from the network, the UE shall stop the timer T3418, if running, and then process the challenge information as normal. If the GUTI/IMSI mapping in the network was correct, the network should terminate the authentication procedure by sending an AUTHENTICATION REJECT message (see clause 5.4.2.5).

 If the network is validated successfully (an AUTHENTICATION REQUEST message that contains a valid SQN and MAC is received), the UE shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430) if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

 If the UE receives the second AUTHENTICATION REQUEST message while T3418 is running, and the MAC value cannot be resolved, the UE shall follow the procedure specified in this clause, item c, starting again from the beginning, or if the message contains a UMTS authentication challenge, the UE shall follow the procedure specified in item d. If the SQN is invalid, the UE shall proceed as specified in item e.



Figure 5.4.2.7.1: Authentication failure procedure (EMM cause #20 "MAC failure" or
#26 "non-EPS authentication unacceptable")

d) Authentication failure (EMM cause #26 "non-EPS authentication unacceptable"):

 The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #26 "non-EPS authentication unacceptable", to the network and start the timer T3418 (see example in figure 5.4.2.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3410, T3417, T3421 or T3430). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause #26 "non-EPS authentication unacceptable", the network may initiate the identification procedure described in clause 5.4.4. This is to allow the network to obtain the IMSI from the UE. The network may then check that the GUTI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the UE shall send the IDENTITY RESPONSE message.

NOTE 2: Upon receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause #26 "non-EPS authentication unacceptable", the network may also terminate the authentication procedure (see clause 5.4.2.5).

 If the GUTI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the UE. Upon receiving the new AUTHENTICATION REQUEST message from the network, the UE shall stop the timer T3418, if running, and then process the challenge information as normal. If the GUTI/IMSI mapping in the network was correct, the network should terminate the authentication procedure by sending an AUTHENTICATION REJECT message (see clause 5.4.2.5).

e) Authentication failure (EMM cause #21 "synch failure"):

 The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #21 "synch failure", to the network and start the timer T3420 (see example in figure 5.4.2.7.2). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3410, T3417, T3421 or T3430). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with the EMM cause #21 "synch failure", the network shall use the returned AUTS parameter from the authentication failure parameter IE in the AUTHENTICATION FAILURE message, to re-synchronise. The re-synchronisation procedure requires the MME to delete all unused authentication vectors for that IMSI and obtain new vectors from the HSS. When re-synchronisation is complete, the network shall initiate the authentication procedure. Upon receipt of the AUTHENTICATION REQUEST message, the UE shall stop the timer T3420, if running.

NOTE 3: Upon receipt of two consecutive AUTHENTICATION FAILURE messages from the UE with EMM cause #21 "synch failure", the network may terminate the authentication procedure by sending an AUTHENTICATION REJECT message.

 If the network is validated successfully (a new AUTHENTICATION REQUEST message is received which contains a valid SQN and MAC) while T3420 is running, the UE shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430), if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

 If the UE receives the second AUTHENTICATION REQUEST message while T3420 is running, and the MAC value cannot be resolved, the UE shall follow the procedure specified in item c or if the message contains a UMTS authentication challenge, the UE shall proceed as specified in item d; if the SQN is invalid, the UE shall follow the procedure specified in this clause, item e, starting again from the beginning.



Figure 5.4.2.7.2: Authentication failure procedure (EMM cause #21 "synch failure")

 Upon receipt of an AUTHENTICATION REJECT message, the UE shall perform the actions as specified in clause 5.4.2.5.

f) Network failing the authentication check:

 If the UE deems that the network has failed the authentication check, then it shall request RRC to locally release the RRC connection and treat the active cell as barred (see 3GPP TS 36.304 [21]). The UE shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430), if they were running and stopped when the UE received the first AUTHENTICATION REQUEST message containing an incorrect authentication challenge data causing the authentication failure.

g) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication from lower layers (if the authentication procedure is triggered by a tracking area updating procedure)

 The UE shall stop any of the timers T3418 and T3420, if running, and re-initiate the tracking area updating procedure.

h) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication with TAI change from lower layers (if the authentication procedure is triggered by a service request procedure)

 The UE shall stop any of the timers T3418 and T3420, if running.

 If the current TAI is not in the TAI list, the authentication procedure shall be aborted and a tracking area updating procedure shall be initiated.

 If the current TAI is still part of the TAI list, it is up to the UE implementation how to re-run the ongoing procedure that triggered the authentication procedure.

i) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication without TAI change from lower layers (if the authentication procedure is triggered by a service request procedure)

 The UE shall stop any of the timers T3418 and T3420, if running. It is up to the UE implementation how to re-run the ongoing procedure that triggered the authentication procedure.

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

 If the AUTHENTICATION REQUEST message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the AUTHENTICATION REQUEST message. If a failure of handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the AUTHENTICATION REQUEST message.

k) Change of cell into a new tracking area

 If a cell change into a new tracking area that is not in the TAI list occurs before the AUTHENTICATION RESPONSE message is sent, the UE may discard sending the AUTHENTICATION RESPONSE message to the network and continue with the initiation of tracking area updating procedure as described in clause 5.5.3.

l) AUTHENTICATION REJECT message is received without integrity protection and none of the timers T3416, T3418 and T3420 is running

 If an AUTHENTICATION REJECT message is received and if none of the timers T3416, T3418 and T3420 is running, then the UE shall discard the AUTHENTICATION REJECT message. Additionally, the UE may request RRC to locally release the RRC connection and treat the active cell as barred (see 3GPP TS 36.304 [21]).

For items c, d, and e if the UE does not have a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services, and it does not have a PDN connection for RLOS established or is establishing a PDN connection for RLOS:

 The UE shall stop timer T3418, if the timer is running and the UE enters EMM-IDLE mode, e.g. upon detection of a lower layer failure, release of the NAS signalling connection, or as the result of an inter-system handover to A/Gb mode, Iu mode or N1 mode.

 The UE shall deem that the network has failed the authentication check or that the source of the authentication challenge is not genuine and proceed as described in item f if any of the following occurs:

- the timer T3418 or T3420 expires;

- the UE detects any combination of the authentication failures: EMM cause #20 "MAC failure", #21 "synch failure", or #26 "non-EPS authentication unacceptable", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only if the authentication challenges causing the second and third authentication failure are received by the UE while the timer T3418 or T3420 started after the previous authentication failure is running.

 [RZ: Can be included in the first paragraph.]

For items c, d, and e if the UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services, or it has a PDN connection for RLOS established or is establishing a PDN connection for RLOS:

1) The UE shall stop timer T3418, if the timer is running and the UE enters EMM-IDLE mode, e.g. upon detection of a lower layer failure, release of the NAS signalling connection, or as the result of an inter-system handover to A/Gb mode, Iu mode or N1 mode.

2) Depending on local requirements or operator preference for emergency bearer services, if the UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services, the MME need not follow the procedures specified for the authentication failure specified in the present clause. The MME may respond to the AUTHENTICATION FAILURE message by initiating the security mode control procedure selecting the "null integrity protection algorithm" EIA0, "null ciphering algorithm" EEA0 or may abort the authentication procedure and continue using the current security context, if any. The MME shall deactivate all non-emergency EPS bearer contexts, if any, by initiating an EPS bearer context deactivation procedure. If there is an ongoing PDN connectivity procedure, the MME shall deactivate all non-emergency EPS bearer contexts upon completion of the PDN connectivity procedure. The network shall consider the UE to be attached for emergency bearer services only.

 If a UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services and sends an AUTHENTICATION FAILURE message to the MME with the EMM cause appropriate for these cases (#20, #21, or #26, respectively) and receives the SECURITY MODE COMMAND message before the timeout of timer T3418 or T3420, the UE shall deem that the network has passed the authentication check successfully, stop timer T3418 or T3420, respectively, and execute the security mode control procedure.

 If a UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services when timer T3418 or T3420 expires, the UE shall not deem that the network has failed the authentication check and not behave as described in item f. Instead the UE shall continue using the current security context, if any, deactivate all non-emergency EPS bearer contexts, if any, by initiating UE requested PDN disconnect procedure. If there is an ongoing PDN connectivity procedure, the UE shall deactivate all non-emergency EPS bearer contexts upon completion of the PDN connectivity procedure.

 The UE shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430) if:

- they were running and stopped when the UE received the AUTHENTICATION REQUEST message and detected an authentication failure; and

- the procedures associated with these timers have not yet been completed.

 The UE shall consider itself to be attached for emergency bearer services only.

3) Depending on local regulation and operator policy, if the UE has a PDN connection for RLOS established or is establishing a PDN connection for RLOS, the MME need not follow the procedures specified for the authentication failure specified in the present clause. The MME may respond to the AUTHENTICATION FAILURE message by initiating the security mode control procedure selecting the "null integrity protection algorithm" EIA0, "null ciphering algorithm" EEA0 or may abort the authentication procedure and continue using the current security context, if any. The network shall consider the UE to be attached for access to RLOS.

 If a UE has a PDN connection for RLOS established or is establishing a PDN connection for RLOS and sends an AUTHENTICATION FAILURE message to the MME with the EMM cause appropriate for these cases (#20, #21, or #26, respectively) and receives the SECURITY MODE COMMAND message before the timeout of timer T3418 or T3420, the UE shall deem that the network has passed the authentication check successfully, stop timer T3418 or T3420, respectively, and execute the security mode control procedure.

 If a UE has a PDN connection for RLOS established or is establishing a PDN connection for RLOS when timer T3418 or T3420 expires, the UE shall not deem that the network has failed the authentication check and not behave as described in item f. Instead the UE shall continue using the current security context, if any.

 The UE shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430) if:

- they were running and stopped when the UE received the AUTHENTICATION REQUEST message and detected an authentication failure; and

- the procedures associated with these timers have not yet been completed.

 The UE shall consider itself to be attached for access to RLOS.