**3GPP TSG-CT WG1 Meeting #137-eC1-225190**

**E-Meeting, 18th – 26th August 2022…………………………………………(was C1-224987)**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **1** | **Current version:** | **17.7.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Clarification when authentication fails |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI18 |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 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:*** | When authentication procedure is deemed not successful, network provides AUTHENTICATION REJECT message to the UE, the UE behaviour is to remove the EMM context. Additionally SIM is considered invalid till power cycle. See below: *“In case of PLMN, the USIM shall be considered invalid until switching off the UE or the UICC containing the USIM is removed”*Given authenticaiton is not successful, network cannot know if its actually a genuine UE. Thus any context at the network should not be impacted of the genuine UESome parts of 24.301 already state that network should keep the EMM context unchanged for example below:*“If a SERVICE REQUEST, EXTENDED SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message fails the integrity check and the UE has only PDN connections for non-emergency bearer services established and the PDN connections are not for RLOS, the MME shall send the SERVICE REJECT message with EMM cause #9 "UE identity cannot be derived by the network" and keep the EMM-context and EPS security context unchanged”* But some other parts this network behaviour is missed to be specified. Thus its proposed to align same behaviour in other places too.  |
|  |  |
| ***Summary of change:*** | Align same behaviour of network keeping the EMM-context if authentication procedure has failed |
|  |  |
| ***Consequences if not approved:*** | "Risk of genuine UE context removal at network" |
|  |  |
| ***Clauses affected:*** | 4.4.4.3, 5.4.2.5, 5.5.1.2.7 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\* Start Change \*\*\*\*\*

#### 4.4.4.3 Integrity checking of NAS signalling messages in the MME

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the MME or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

- EMM messages:

- ATTACH REQUEST;

- IDENTITY RESPONSE (if requested identification parameter is IMSI);

- AUTHENTICATION RESPONSE;

- AUTHENTICATION FAILURE;

- SECURITY MODE REJECT;

- DETACH REQUEST;

- DETACH ACCEPT;

- TRACKING AREA UPDATE REQUEST.

NOTE 1: The TRACKING AREA UPDATE REQUEST message is sent by the UE without integrity protection, if the tracking area updating procedure is initiated due to an inter-system change in idle mode and no current EPS security context is available in the UE. The other messages are accepted by the MME without integrity protection, as in certain situations they are sent by the UE before security can be activated.

NOTE 2: The DETACH REQUEST message can be sent by the UE without integrity protection, e.g. if the UE is attached for emergency bearer services or access to RLOS and there is no shared EPS security context available, or if due to user interaction an attach procedure is cancelled before the secure exchange of NAS messages has been established. For these cases the network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic tracking area updating or still responding to paging) before marking the UE as EMM-DEREGISTERED.

All ESM messages are integrity protected except a PDN CONNECTIVITY REQUEST message if it is sent piggybacked in ATTACH REQUEST message and NAS security is not activated.

Once a current EPS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM entity in the MME shall process the following NAS signalling messages, even if the MAC included in the message fails the integrity check or cannot be verified, as the EPS security context is not available in the network:

- ATTACH REQUEST;

- IDENTITY RESPONSE (if requested identification parameter is IMSI);

- AUTHENTICATION RESPONSE;

- AUTHENTICATION FAILURE;

- SECURITY MODE REJECT;

- DETACH REQUEST;

- DETACH ACCEPT;

- TRACKING AREA UPDATE REQUEST;

- SERVICE REQUEST;

- EXTENDED SERVICE REQUEST;

- CONTROL PLANE SERVICE REQUEST.

NOTE 3: These messages are processed by the MME even when the MAC that fails the integrity check or cannot be verified, as in certain situations they can be sent by the UE protected with an EPS security context that is no longer available in the network.

If an ATTACH REQUEST message is received without integrity protection or fails the integrity check and it is not an attach request for emergency bearer services and it is not an attach request for access to RLOS, the MME shall authenticate the subscriber before processing the attach request any further. Additionally, if the MME initiates a security mode control procedure, the MME shall include a HASHMME IE in the SECURITY MODE COMMAND message as specified in clause 5.4.3.2. If authentication procedure is not successful the MME shall maintain, if any, the EMM-context and EPS security context unchanged. For the case when the attach procedure is for emergency bearer services see clause 5.5.1.2.3 and clause 5.4.2.5.

If a DETACH REQUEST message fails the integrity check, the MME shall proceed as follows:

- If it is not a detach request due to switch off, and the MME can initiate an authentication procedure, the MME should authenticate the subscriber before processing the detach request any further.

- If it is a detach request due to switch off, or the MME does not initiate an authentication procedure for any other reason, the MME may ignore the detach request and remain in state EMM-REGISTERED.

NOTE 4: The network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic tracking area updating or still responding to paging) before marking the UE as EMM-DEREGISTERED.

If a TRACKING AREA UPDATE REQUEST message is received without integrity protection or fails the integrity check and the UE provided a nonceUE, GPRS ciphering key sequence number, P-TMSI and RAI in the TRACKING AREA UPDATE REQUEST message, the MME shall initiate a security mode control procedure to take a new mapped EPS security context into use; otherwise, if the UE has only a PDN connection for non-emergency bearer services established and the PDN connection is not for RLOS, the MME shall initiate an authentication procedure. Additionally, if the MME initiates a security mode control procedure, the MME shall include a HASHMME IE in the SECURITY MODE COMMAND message as specified in clause 5.4.3.2. If authentication procedure is not successful the MME shall maintain, if any, the EMM-context and EPS security context unchanged. For the case when the UE has a PDN connection for emergency bearer services or for RLOS see clause 5.5.3.2.3 and clause 5.4.2.5.

If a SERVICE REQUEST, EXTENDED SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message fails the integrity check and the UE has only PDN connections for non-emergency bearer services established and the PDN connections are not for RLOS, the MME shall send the SERVICE REJECT message with EMM cause #9 "UE identity cannot be derived by the network" and keep the EMM-context and EPS security context unchanged. For the case when the UE has a PDN connection for emergency bearer services or RLOS and integrity check fails, the MME may skip the authentication procedure even if no EPS security context is available and proceed directly to the execution of the security mode control procedure as specified in clause 5.4.3. After successful completion of the service request procedure, the network shall deactivate all non-emergency EPS bearers locally which are not EPS bearers for RLOS. The emergency EPS bearers shall not be deactivated. The network may deactivate the EPS bearers for RLOS.

Once the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM or ESM entity in the MME shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If any NAS signalling message, having not successfully passed the integrity check, is received, then the NAS in the MME shall discard that message. If any NAS signalling message is received, as not integrity protected even though the secure exchange of NAS messages has been established, then the NAS shall discard this message.

\*\*\*\*\* Next Change \*\*\*\*\*

#### 5.4.2.5 Authentication not accepted by the network

If the authentication response (RES) returned by the UE is not valid, the network response depends upon the type of identity used by the UE in the initial NAS message, that is:

- if the GUTI was used; or

- if the IMSI was used.

If the GUTI was used, the network should initiate an identification procedure. If the IMSI given by the UE during the identification procedure differs from the IMSI the network had associated with the GUTI, the authentication should be restarted with the correct parameters. Otherwise, if the IMSI provided by the UE is the same as the IMSI stored in the network (i.e. authentication has really failed), the network should send an AUTHENTICATION REJECT message to the UE.

If the IMSI was used for identification in the initial NAS message, or the network decides not to initiate the identification procedure after an unsuccessful authentication procedure, the network should send an AUTHENTICATION REJECT message to the UE. The network shall maintain, if any, the EMM-context and EPS security context unchanged.

Upon receipt of an AUTHENTICATION REJECT message,

a) if the message has been successfully integrity checked by the NAS, the UE shall set the update status to EU3 ROAMING NOT ALLOWED, delete the stored GUTI, TAI list, last visited registered TAI and KSIASME. The USIM shall be considered invalid until switching off the UE or the UICC containing the USIM is removed. If the UE maintains a counter for "SIM/USIM considered invalid for GPRS services", then the UE shall set this counter to UE implementation-specific maximum value. If the UE maintains a counter for "SIM/USIM considered invalid for non-GPRS services", then the UE shall set this counter to UE implementation-specific maximum value.

 If A/Gb or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and the MM parameters update status, TMSI, LAI and ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the authentication and ciphering procedure is not accepted by the network; and

 if the UE is operating in single-registration mode, the UE shall in addition handle the 5GMM parameters 5GMM state, 5GS update status, 5G-GUTI, last visited registered TAI, TAI list and ngKSI as specified in 3GPP TS 24.501 [54] for the case when the authentication procedure performed over 3GPP access is not accepted by the network; and

b) if the message is received without integrity protection and if timer T3416, T3418 or T3420 is running, the UE shall start timer T3247 (see 3GPP TS 24.008 [13]) with a random value uniformly drawn from the range between 30 minutes and 60 minutes, if the timer is not running (see clause 5.3.7b). Additionally, the UE shall:

- if the UE maintains a counter for "SIM/USIM considered invalid for GPRS services" events and the counter has a value less than a UE implementation-specific maximum value, proceed as specified in clause 5.3.7b, list item 1a for the case that the EMM cause value received is #3; and

- otherwise proceed as specified under list item a above for the case that the message has been successfully integrity checked.

If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any EMM signalling procedure, stop any of the timers T3410, T3416, T3417, T3430, T3421, T3418 or T3420 (if they were running) and enter state EMM-DEREGISTERED.

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 in the present clause. The MME may continue a current EMM specific procedure or PDN connectivity request procedure. Upon completion of the authentication procedure, if not initiated as part of another procedure, or upon completion of the EMM procedure or PDN connectivity request procedure, the MME shall deactivate all non-emergency EPS bearers, if any, by initiating an EPS bearer context deactivation procedure. The network shall consider the UE to be attached for emergency bearer services only.

Depending on local regulation and operator policy, if the UE is requesting attach for access to RLOS, the MME need not follow the procedures specified for the authentication failure in the present clause. The MME may continue a current EMM specific procedure.

\*\*\*\*\* Next Change \*\*\*\*\*

##### 5.5.1.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

 If a lower layer failure occurs before the message ATTACH COMPLETE has been received from the UE, the network shall locally abort the attach procedure, enter state EMM-DEREGISTERED and shall not resend the message ATTACH ACCEPT. If a new GUTI was assigned to the UE in the attach procedure, the MME shall consider both the old and the new GUTI as valid until the old GUTI can be considered as invalid by the network or the EMM context which has been marked as detached in the network is released.

 If the old GUTI was allocated by an MME other than the current MME, the current MME does not need to retain the old GUTI. If the old GUTI is used by the UE in a subsequent attach message, the network may use the identification procedure to request the UE's IMSI.

b) Protocol error

 If the ATTACH REQUEST message is received with a protocol error, the network shall return an ATTACH REJECT message with one of the following EMM cause values:

 #96: invalid mandatory information;

 #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 ATTACH ACCEPT message and shall reset and restart timer T3450.

 This retransmission is repeated four times, i.e. on the fifth expiry of timer T3450, the attach procedure shall be aborted and the MME enters state EMM-DEREGISTERED. If a new GUTI was allocated in the ATTACH ACCEPT message, the network shall consider both the old and the new GUTI as valid until the old GUTI can be considered as invalid by the network or the EMM context which has been marked as detached in the network is released. If the old GUTI was allocated by an MME other than the current MME, the current MME does not need to retain the old GUTI.

 If the old GUTI is used by the UE in a subsequent attach message, the network acts as specified for case a above.

d) ATTACH REQUEST received after the ATTACH ACCEPT message has been sent and before the ATTACH COMPLETE message is received

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

- if the information elements do not differ, then the ATTACH ACCEPT message shall be resent and the timer T3450 shall be restarted if an ATTACH COMPLETE message is expected. In that case, the retransmission counter related to T3450 is not incremented.

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

- If one or more of the information elements in the ATTACH REQUEST message differs from the ones received within the previous ATTACH REQUEST message, the previously initiated attach procedure shall be aborted and the new attach procedure shall be executed;

- if the information elements do not differ, then the network shall continue with the previous attach procedure and shall ignore the second ATTACH REQUEST message.

f) ATTACH REQUEST received in state EMM-REGISTERED

 If an ATTACH REQUEST message is received in state EMM-REGISTERED the network may initiate the EMM common procedures; if it turned out that the ATTACH REQUEST message was sent by a genuine UE that has already been attached, the EMM context, EPS bearer contexts, if any, are deleted and the new ATTACH REQUEST is progressed, otherwise if network considers ATTACH REQUEST message was not sent by a genuine UE based on authentication procedure the network shall maintain the EMM-context, if any, unchanged.

NOTE 1: The network can determine that the UE is genuine by executing the authentication procedure as described in clause 5.4.2.

g) TRACKING AREA UPDATE REQUEST message received before ATTACH COMPLETE message.

 Timer T3450 shall be stopped. The allocated GUTI in the attach procedure shall be considered as valid and the tracking area updating procedure shall be rejected with the EMM cause #10 "implicitly detached" as described in clause 5.5.3.2.5.

h) DETACH REQUEST message received before ATTACH COMPLETE message.

 The network shall abort the attach procedure and shall progress the detach procedure as described in clause 5.5.2.2.

i) If EMM-REGISTERED without PDN connection is supported by the UE and the MME, the MME receives an ATTACH REQUEST message with an ESM message included in the ESM message container information element, and the ESM sublayer in the MME detects a message error according to clause 7, the MME may decide to proceed with the attach procedure or to reject it. When sending the ATTACH ACCEPT or ATTACH REJECT message to the UE, the MME shall include the ESM message provide by the ESM layer in the ESM message container information element.

j) UE security capabilities invalid or unacceptable

 If the ATTACH REQUEST message is received with invalid or unacceptable UE security capabilities (e.g. no EPS encryption algorithms (all bits zero), no EPS integrity algorithms (all bits zero), mandatory EPS encryption algorithms not supported or mandatory EPS integrity algorithms not supported, etc.), the MME shall return an ATTACH REJECT message.

NOTE 2: EMM cause value to be used in ATTACH REJECT message is up to the network implementation.

\*\*\*\*\* End Change \*\*\*\*\*