**3GPP TSG-CT WG1 Meeting #130-eC1-21xxxx**

**Electronic meeting, 20-28 May 2021 (Revision of C1-212954)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.301** | **CR** | **3524** | **rev** | **1** | **Current version:** | **17.2.0** |  |
|  | | | | | | | | |
| *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:*** | Add 5GMM SR procedure for non-integrity protected reject message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | OPPO | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2021-5-6 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | For EMM, when UE receives the ATTACH REJECT, TAU REJECT and SERVICE REJECT messages without integrity protection, as in clause 5.3.7b, if UE is in single-registration mode, UE should also handle the 5GMM parameters as the same 5GMM rejection cause values specified in TS 24.501.  However, for handling 5GMM parameters, it is only mentioned registration procedures without service request procedure.  Meanwhile, the 5GMM parameters handling is already in clause 5.6.1.5 Service request procedure not accepted by the network, for exmaple:  For the EMM cause value #3 or #6, if the UE is operating in single-registration mode, the UE shall 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 service request procedure performed over 3GPP access is rejected with the 5GMM cause with the same value.  This handling is already applied to 4G and 3G as below:  - if A/Gb mode or Iu mode is supported by the UE, handle the GMM parameters GPRS attach attempt counter, routing area updating attempt counter or service request attempt counter, GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the GPRS attach, routing area updating or service request procedure is rejected with the GMM cause of the same value in a NAS message without integrity protection;  Also the service request attempt counter is missing in the 5GMM parameters since in 24.501 there is the following:  On receipt of the SERVICE REJECT message, if the UE is in state 5GMM-SERVICE-REQUEST-INITIATED, the UE shall reset the service request attempt counter and stop timer T3517 if running. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add 5GMM service request procedure and service request attempt counter when UE in single-registration mode receives non-integrity protected MM reject messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 5GMM the service request procedure and service request attempt counter are missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.7b | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*

### 5.3.7b Specific requirements for UE when receiving non-integrity protected reject messages

This subclause specifies the requirements for a UE that is not configured to use timer T3245 (see 3GPP TS 24.368 [15A] or 3GPP TS 31.102 [17]) and receives an ATTACH REJECT, TRACKING AREA UPDATE REJECT or SERVICE REJECT message without integrity protection with specific EMM causes.

NOTE 1: Additional UE requirements for this case, requirements for other EMM causes, and requirements for the case when the UE receives an integrity protected reject message are specified in subclauses 5.5.1, 5.5.3 and 5.6.1.

The UE may maintain a list of PLMN-specific attempt counters and a list of PLMN-specific PS-attempt counters (see 3GPP TS 24.008 [13]). The maximum number of possible entries in each list is implementation dependent.

Additionally, the UE may maintain one counter for "SIM/USIM considered invalid for non-GPRS services" events and one counter for "SIM/USIM considered invalid for GPRS services" events (see 3GPP TS 24.008 [13]).

If the UE receives an ATTACH REJECT, TRACKING AREA UPDATE REJECT or SERVICE REJECT message without integrity protection with EMM cause value #3, #6, #7, #8, #11, #12, #13, #14, #15, #31 or #35 before the network has established secure exchange of NAS messages for the NAS signalling connection, 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, and take the following actions:

1) if the EMM cause value received is #3, #6, #7 or #8, and

a) 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, the UE shall:

i) set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and eKSI;

- delete the list of equivalent PLMNs;

- increment the counter for "SIM/USIM considered invalid for GPRS services" events;

- if the EMM cause value received is #3, #6 or #8, and if the UE maintains a counter for "SIM/USIM considered invalid for non-GPRS services" and the counter has a value less than a UE implementation-specific maximum value, increment the counter;

- if an attach, tracking area updating or a service request procedure was performed, reset the attach attempt counter, the tracking area updating attempt counter or the service request attempt counter, respectively;

- if A/Gb mode or Iu mode is supported by the UE, handle the GMM parameters GPRS attach attempt counter, routing area updating attempt counter or service request attempt counter, GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the GPRS attach, routing area updating or service request procedure is rejected with the GMM cause of the same value in a NAS message without integrity protection;

- If the UE is operating in single-registration mode and the EMM cause value received is #3, #6 or #7, the UE shall in addition handle the 5GMM parameters 5GMM state, 5GS update status, registration attempt counter or service request attempt counter, 5G-GUTI, last visited registered TAI, TAI list and ngKSI as specified in 3GPP TS 24.501 [54] for the case when the registration request or service request procedure performed over 3GPP access is rejected with the 5GMM cause with the same value in a NAS message without integrity protection.

- If the UE is operating in single-registration mode and the EMM cause value received is #8, the UE shall in addition set the 5GMM state to 5GMM-DEREGISTERED, the 5GS update status to 5U3 ROAMING NOT ALLOWED, shall reset the registration attempt counter and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI for 3GPP access.

- store the current TAI in the list of "forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "forbidden tracking areas for roaming" for non-integrity protected NAS reject message and enter the state EMM-DEREGISTERED.LIMITED-SERVICE; and

- search for a suitable cell in another tracking area or in another location area according to 3GPP TS 36.304 [21]; or

ii) proceed as specified in subclauses 5.5.1, 5.5.3 and 5.6.1;

- increment the counter for "SIM/USIM considered invalid for GPRS services" events; and

- if the EMM cause value received is #3, #6 or #8, and if the UE maintains a counter for "SIM/USIM considered invalid for non-GPRS services" and the counter has a value less than a UE implementation specific maximum value, increment the counter; and

b) else the UE shall proceed as specified in subclauses 5.5.1, 5.5.3 and 5.6.1;

2) if the EMM cause value received is #12, #13 or #15, the UE shall additionally proceed as specified in subclauses 5.5.1, 5.5.3 and 5.6.1;

3) if the EMM cause value received is #11, #14 or #35 and the UE is in its HPLMN or EHPLMN (if the EHPLMN list is present),

- the UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and eKSI. The UE shall delete the list of equivalent PLMNs. Additionally, if an attach, tracking area updating or service request procedure was performed, the UE shall reset the attach attempt counter or the tracking area updating attempt counter or the service request attempt counter, respectively.

- if A/Gb mode 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, GPRS ciphering key sequence number and GPRS attach attempt counter or routing area updating attempt counter or service request attempt counter as specified in 3GPP TS 24.008 [13] for the case when the procedure is rejected with the GMM cause with the same value in a NAS message without integrity protection;

- If the UE is operating in single-registration mode and the EMM cause value received is #11, the UE shall in addition handle the 5GMM parameters 5GMM state, 5GS update status, registration attempt counter or service request attempt counter, 5G-GUTI, last visited registered TAI, TAI list and ngKSI as specified in 3GPP TS 24.501 [54] for the case when the registration request procedure or service request procedure performed over 3GPP access is rejected with the 5GMM cause with the same value in a NAS message without integrity protection.

- If the UE is operating in single-registration mode and the EMM cause value received is #14 or #35, the UE shall in addition set the 5GMM state to 5GMM-DEREGISTERED, the 5GS update status to 5U3 ROAMING NOT ALLOWED, shall reset the registration attempt counter and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI for 3GPP access.

- the UE shall store the current TAI in the list of "forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "forbidden tracking areas for roaming" for non-integrity protected NAS reject message and enter the state EMM-DEREGISTERED.LIMITED-SERVICE; and

- the UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21];

4) if the EMM cause value received is #11 or #35 and the UE is not in its HPLMN or EHPLMN (if the EHPLMN list is present), in addition to the UE requirements specified in subclause 5.5.1, 5.5.3 and 5.6.1,

if the UE maintains a list of PLMN-specific attempt counters and the PLMN-specific attempt counter for the PLMN sending the reject message has a value less than a UE implementation-specific maximum value, the UE shall increment the PLMN-specific attempt counter for the PLMN;

5) if the EMM cause value received is #14 and the UE is not roaming in its HPLMN or EHPLMN (if the EHPLMN list is present), in addition to the UE requirements specified in subclause5.5.1, 5.5.3 and 5.6.1,

if the UE maintains a list of PLMN-specific PS-attempt counter and the PLMN-specific PS-attempt counter of the PLMN sending the reject message has a value less than a UE implementation-specific maximum value, the UE shall increment the PS-attempt counter of the PLMN; and

6) if the EMM cause value received is #31 for a UE that has indicated support for CIoT optimizations, the UE may discard the message or alternatively the UE should:

- set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3);

- store the current TAI in the list of "forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "forbidden tracking areas for roaming" for non-integrity protected NAS reject message; and

- search for a suitable cell in another tracking area according to 3GPP TS 36.304 [21].

Upon expiry of timer T3247, the UE shall

- remove all tracking areas from the list of "forbidden tracking areas for regional provision of service" and the list of "forbidden tracking areas for roaming", which were stored in these lists for non-integrity protected NAS reject message;

- set the USIM to valid for EPS services, if

- the UE does not maintain a counter for "SIM/USIM considered invalid for GPRS services" events; or

- the UE maintains a counter for "SIM/USIM considered invalid for GPRS services" events and this counter has a value less than a UE implementation-specific maximum value;

- set the USIM to valid for non-EPS services, if

- the UE does not maintain a counter for "SIM/USIM considered invalid for non-GPRS services" events; or

- the UE maintains a counter for "SIM/USIM considered invalid for non-GPRS services" events and this counter has a value less than a UE implementation-specific maximum value;

- if the UE maintains a list of PLMN-specific attempt counters, for each PLMN-specific attempt counter that has a value greater than zero and less than a UE implementation-specific maximum value, remove the respective PLMN from the forbidden PLMN list;

- if the UE maintains a list of PLMN-specific PS-attempt counters, for each PLMN-specific PS-attempt counter that has a value greater than zero and less than a UE implementation-specific maximum value, remove the respective PLMN from the "forbidden PLMNs for GPRS service" list. If the resulting "forbidden PLMNs for GPRS service" list is empty, the UE shall re-enable the E-UTRA capability (see subclause 4.5);

- if the UE is supporting A/Gb mode or Iu mode, perform the actions as specified in 3GPP TS 24.008 [13] for the case when timer T3247 expires;

- if the UE is supporting N1 mode, perform the actions as specified in 3GPP TS 24.501 [54], subclause 5.3.20.2 for the case when timer T3247 expires; and

- initiate an EPS attach procedure or tracking area updating procedure, if still needed, dependent on EMM state and EPS update status, or perform PLMN selection according to 3GPP TS 23.122 [6].

If the UE maintains a list of PLMN-specific attempt counters and PLMN-specific PS-attempt counters, when the UE is switched off, the UE shall, for each PLMN-specific attempt counter that has a value greater than zero and less than the UE implementation-specific maximum value, remove the respective PLMN from the forbidden PLMN list. When the USIM is removed, the UE should perform this action.

The PLMN-specific attempt counter and the PLMN-specific PS-attempt counter shall be reset when the UICC containing the USIM is removed or the PLMN is added to a list of "forbidden PLMNs" in the USIM as specified in 3GPP TS 23.122 [6].

NOTE 2: If the respective PLMN was stored in the extension of the "forbidden PLMNs" list, then according to 3GPP TS 23.122 [6] the UE will delete the contents of this extension when the USIM is removed.

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