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

**Electronic meeting, 20-28 May 2021 (Revision of C1-212943)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3175** | **rev** | **1** | **Current version:** | **17.2.1** |  |
|  |
| *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:***  | Add EMM 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 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:*** | For 5GMM, when UE receives the REGISTRATION REJECT and SERVICE REJECT messages without integrity protection, as in clause 5.3.20.2, if UE is in single-registration mode, UE should also handle the EMM parameters as the same EMM rejection cause values specified in TS 24.301.However, for handling EMM parameters, it is only mentioned attach, TAU procedures without service request procedure.Meanwhile, the EMM parameters handling is already in clause 5.6.1.5 Service request procedure not accepted by the network, for exmaple: If the message was received via 3GPP access and the UE is operating in the single-registration mode, the UE shall handle the EMM parameters EMM state, EPS update status, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the service request procedure is rejected with the EMM cause with the same value. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed. If the message has been successfully integrity checked by the NAS and 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.Also the service request attempt counter is missing in the EMM parameters since in 24.301 there is the following:On receipt of the SERVICE REJECT message, if the UE is in state EMM-SERVICE-REQUEST-INITIATED and the message is integrity protected or contains a reject cause other than EMM cause value #25, the UE shall reset the service request attempt counter, stop timer T3417, T3417ext or T3417ext-mt, if running. |
|  |  |
| ***Summary of change:*** | Add EMM 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:*** | EMM the service request procedure and service request attempt counter are missing. |
|  |  |
| ***Clauses affected:*** | 5.3.20.2 |
|  |  |
|  | **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 \*\*\*\*\*

#### 5.3.20.2 Requirements for UE in a PLMN

The UE shall maintain:

- a list of PLMN-specific attempt counters (see 3GPP TS 24.301 [15]). The maximum number of possible entries in the list is implementation dependent. This list is applicable to access attempts via 3GPP access only;

- a list of PLMN-specific attempt counters for non-3GPP access, if the UE supports non-3GPP access. The maximum number of possible entries in the list is implementation dependent. This list is applicable to access attempts via non-3GPP access only;

- a list of PLMN-specific N1 mode attempt counters for 3GPP access. The maximum number of possible entries in the list is implementation dependent. This list is applicable to access attempts via 3GPP access only;

- a list of PLMN-specific N1 mode attempt counters for non-3GPP access, if the UE supports non-3GPP access. The maximum number of possible entries in the list is implementation dependent. This list is applicable to access attempts via non-3GPP access only;

- one counter for "SIM/USIM considered invalid for GPRS services" events (see 3GPP TS 24. 008 [12]); and

- one counter for "USIM considered invalid for 5GS services over non-3GPP access" events, if the UE supports non-3GPP access.

A UE supporting non-EPS services shall maintain one counter for "SIM/USIM considered invalid for non-GPRS services" events (see 3GPP TS 24.008 [12]).

The UE shall store the above lists of attempt counters and the event counters in its non-volatile memory. The UE shall erase the lists and reset the event counters to zero when the UICC containing the USIM is removed. The counter values shall not be affected by the activation or deactivation of MICO mode or power saving mode (see 3GPP TS 24.301 [15]).

The UE implementation-specific maximum value for any of the above counters shall not be greater than 10.

NOTE 1: Different counters can use different UE implementation-specific maximum values.

If the UE receives a REGISTRATION REJECT or SERVICE REJECT message without integrity protection with 5GMM cause value #3, #6, #7, #11, #12, #13, #15, #27, #31, #62, #72 or #73 before the network has established secure exchange of NAS messages for the N1 NAS signalling connection, the UE shall stop timer T3510 or T3517 if running, and start timer T3247 (see 3GPP TS 24.008 [12]) 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 5GMM cause value received is #3, #6 or #7, and:

a) if the 5GMM cause value is received over 3GPP access, the UE shall:

i) if the UE is already registered over another access:

- store the current TAI in the list of "5GS forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "5GS forbidden tracking areas for roaming" for non-integrity protected NAS reject message and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE; and

- search for a suitable cell in another tracking area according to 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C]; or

ii) otherwise, if the counter for "SIM/USIM considered invalid for GPRS services" events has a value less than a UE implementation-specific maximum value,

- set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI for 3GPP access;

- if the 5GMM cause value received is #3 or #6, delete the list of equivalent PLMNs if any;

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

- if the 5GMM cause value received is #3 or #6, and if the counter for "SIM/USIM considered invalid for non-GPRS services" events has a value less than a UE implementation-specific maximum value, increment the counter;

- if a registration procedure was performed, reset the registration attempt counter and if a service request procedure was performed, reset the service request attempt counter;

- if the UE is operating in single-registration mode, handle the EMM parameters EMM state, EPS update status, EPS attach attempt counter, tracking area updating attempt counter or service request attempt counter, 4G-GUTI, TAI list, eKSI as specified in 3GPP TS 24.301 [15] for the case when the EPS attach, tracking area updating procedure or service request procedure is rejected with the EMM cause of the same value in a NAS message without integrity protection;

- store the current TAI in the list of "5GS forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "5GS forbidden tracking areas for roaming" for non-integrity protected NAS reject message and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE; and

- search for a suitable cell in another tracking area according to 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C]; and as a UE implementation option, the UE may perform registration attempt over the non-3GPP access, if non-3GPP access is available, and the USIM is not considered invalid for 5GS services over non-3GPP access; and

iii) otherwise proceed as specified in subclauses 5.5.1 and 5.6.1;

b) if the 5GMM cause value is received over non-3GPP access, the UE shall:

i) if the UE is already registered over another access:

- enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE; and

- may perform registration attempt over the non-3GPP access if another access point for non-3GPP access is available; or

ii) otherwise, if the counter for "USIM considered invalid for 5GS services over non-3GPP access" events has a value less than a UE implementation-specific maximum value,

- set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete the 5G-GUTI, last visited registered TAI, TAI list and ngKSI for non-3GPP access;

- enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE;

- increment the counter for "USIM considered invalid for 5GS services over non-3GPP access" events; and as a UE implementation option, the UE may either perform registration attempt over the non-3GPP access if another access point for non-3GPP access is available, or if 3GPP access is available, and the SIM/USIM is not considered invalid for 5GS services over 3GPP access, perform registration attempt over the 3GPP access; and

NOTE 2: How to select another access point for non-3GPP access is implementation specific.

iii) otherwise proceed as specified in subclauses 5.5.1 and 5.6.1;

2) if the 5GMM cause value received is #12, #13 or #15, the UE shall proceed as specified in subclauses 5.5.1 and 5.6.1. Additionally, the UE may:

a) if the 5GMM cause value is received over 3GPP access, non-3GPP access is available, the UE is not registered over non-3GPP access yet, and the USIM is not considered invalid for 5GS services over non-3GPP access, perform registration attempt over the non-3GPP access; or

b) if the 5GMM cause value is received over non-3GPP access, 3GPP access is available, the UE is not registered over 3GPP access yet, and the USIM is not considered invalid for 5GS services over 3GPP access, perform registration attempt over the 3GPP access;

3) if the 5GMM cause value received is #11 or #73 and the UE is in its HPLMN or EHPLMN:

a) if the 5GMM cause value is received over 3GPP access, the UE shall:

- set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete, the 5G-GUTI, last visited registered TAI, TAI list, ngKSI for 3GPP access and the list of equivalent PLMNs. Additionally, if a registration procedure was performed, the UE shall reset the registration attempt counter and if a service request procedure was performed, reset the service request attempt counter;

- if the 5GMM cause value received is #11 and the UE is operating in single-registration mode, handle the EMM parameters EMM state, EPS update status, EPS attach attempt counter, tracking area updating attempt counter or service request attempt counter, 4G-GUTI, TAI list, eKSI as specified in 3GPP TS 24.301 [15] for the case when the EPS attach, tracking area updating procedure or service request procedure is rejected with the EMM cause of the same value in a NAS message without integrity protection;

- if the 5GMM cause value received is #73 and the UE is operating in single-registration mode, the UE shall in addition set the EPS update status to EU3 ROAMING NOT ALLOWED and shall delete any 4G-GUTI, last visited registered TAI, TAI list and eKSI. Additionally, the UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED;

- store the current TAI in the list of "5GS forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "5GS forbidden tracking areas for roaming" for non-integrity protected NAS reject message and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE; and

- search for a suitable cell in another tracking area according to 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C]; and as a UE implementation option, the UE may perform registration attempt over the non-3GPP access, if non-3GPP access is available, the UE is not registered over non-3GPP access yet, and the USIM is not considered invalid for 5GS services over non-3GPP access;

b) if the 5GMM cause value is received over non-3GPP access, the UE shall:

- set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete the 5G-GUTI, last visited registered TAI, TAI list and ngKSI for non-3GPP access. Additionally, if a registration procedure was performed, the UE shall reset the registration attempt counter and if a service request procedure was performed, reset the service request attempt counter; and

- enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE. As a UE implementation option, the UE may perform registration attempt over the non-3GPP access if another access point for non-3GPP access is available, or if 3GPP access is available, the UE is not registered over 3GPP access yet, and the USIM is not considered invalid for 5GS services over 3GPP access, perform registration attempt over the 3GPP access;

4) if the 5GMM cause value received is #11 or #73 and the UE is not in its HPLMN or EHPLMN, in addition to the UE requirements specified in subclause 5.5.1 and 5.6.1:

- if the message was received via 3GPP access and if 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; or

- if the message was received via non-3GPP access and if the PLMN-specific attempt counter for non-3GPP access 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 non-3GPP access for the PLMN;

5) if the 5GMM cause value received is #27, the UE shall proceed as specified in subclauses 5.5.1 and 5.6.1. Additionally, if the PLMN-specific N1 mode attempt counter for the respective access type and for the PLMN sending the reject message has a value less than a UE implementation-specific maximum value, the UE shall increment this counter for the PLMN;

6) if the 5GMM cause value received is #72, the UE shall proceed as specified in subclauses 5.5.1 and 5.6.1. Additionally, if the PLMN-specific N1 mode attempt counter for non-3GPP access for the PLMN sending the reject message has a value less than a UE implementation-specific maximum value, the UE shall increment this counter for the PLMN;

7) if the 5GMM 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 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2);

- store the current TAI in the list of "5GS forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "5GS 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 38.304 [28] or 3GPP TS 36.304 [25C]; and

8) if the 5GMM cause value received is #62, the UE may discard the message or alternatively the UE should:

- set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2);

- store the current TAI in the list of "5GS forbidden tracking areas for roaming", memorize the current TAI was stored in the list of "5GS 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 38.304 [28] or 3GPP TS 36.304 [25C].

Upon expiry of timer T3247, the UE shall:

- remove all tracking areas from the list of "5GS forbidden tracking areas for regional provision of service" and the list of "5GS forbidden tracking areas for roaming", which were stored in these lists for non-integrity protected NAS reject message;

- set the USIM to valid for 5GS services for 3GPP access, if:

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

- set the USIM to valid for 5GS services for non-3GPP access, if:

- the counter for "USIM considered invalid for 5GS services over non-3GPP access" events has a value less than a UE implementation-specific maximum value;

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

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

- 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 list of "forbidden PLMNs";

- for each PLMN-specific attempt counter for non-3GPP access that has a value greater than zero and less than a UE implementation-specific maximum value, remove the respective PLMN from the list of "forbidden PLMNs for non-3GPP access to 5GCN";

- re-enable the N1 mode capability for 3GPP access and, for each PLMN-specific N1 mode attempt counter for 3GPP access that has a value greater than zero and less than a UE implementation-specific maximum value, remove the respective PLMN from the list of PLMNs where N1 mode is not allowed for 3GPP access (see 3GPP TS 23.122 [5]);

- re-enable the N1 mode capability for non-3GPP access and, for each PLMN-specific N1 mode attempt counter for non-3GPP access that has a value greater than zero and less than a UE implementation-specific maximum value, remove the respective PLMN from the list of PLMNs where N1 mode is not allowed for non-3GPP access;

- if the UE is supporting A/Gb mode or Iu mode, perform the actions as specified in 3GPP TS 24.008 [12] for the case when timer T3247 expires;

- if the UE is supporting S1 mode, perform the actions as specified in 3GPP TS 24.301 [15] for the case when timer T3247 expires; and

- initiate a registration procedure, if still needed, dependent on 5GMM state and 5GS update status, or perform PLMN selection according to 3GPP TS 23.122 [5].

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 list of "forbidden PLMNs". When the USIM is removed, the UE should perform this action.

When the UE is switched off, the UE shall, for each PLMN-specific attempt counter for non-3GPP access that has a value greater than zero and less than the UE implementation-specific maximum value, remove the respective PLMN from the list of "forbidden PLMNs for non-3GPP access to 5GCN". When the USIM is removed, the UE should perform this action.

NOTE 3: If the respective PLMN was stored in the extension of the "forbidden PLMNs" list, then according to 3GPP TS 23.122 [5] the UE will delete the contents of this extension when the USIM is removed.

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