**3GPP TSG-CT WG1 Meeting #134-eC1-22xxxx**

**E-Meeting, 17th – 25th February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.301** | **CR** | **3728** | **rev** | **1** | **Current version:** | **17.5.0** |  |
|  |
| *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:***  | Correction on reset of PLMN-specific attempt counter |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-02-10 |
|  |  |  |  |  |
| ***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 per TS 24.301 sub 5.3.7b:"*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].*"Based on forbidden PLMNs handling as specified in TS 23.122 sub 3.1 as below (see green text), the UE shall add a PLMN into **the list of "forbidden PLMNs" in the USIM** when the PLMN-specific attempt counter for that VPLMN is **equal to** the MS implementation specific maximum value."*A VPLMN is added to a list of "forbidden PLMNs" in the SIM and thereafter that VPLMN will not be accessed except for disaster roaming services, by the MS when in automatic mode if a message with cause value "PLMN not allowed" or "Requested service option not authorized in this PLMN" or "Serving network not authorized" is received by an MS in response to an LR request from that VPLMN and:**- the MS is configured to use timer T3245 as defined in 3GPP TS 24.008 [23], 3GPP TS 24.301 [23A], and 3GPP TS 24.501 [64];**- the MS is not configured to use timer T3245 and the message is integrity-protected;**- the MS is not configured to use timer T3245, the message is not integrity-protected and the MS does not maintain a list of PLMN-specific attempt counters; or**- the MS is not configured to use timer T3245, the message is not integrity-protected, the MS maintains a list of PLMN-specific attempt counters and the value of the PLMN-specific attempt counter for that VPLMN is* *equal to* *the MS implementation specific maximum value as defined in 3GPP TS 24.008 [23], 3GPP TS 24.301 [23A] and 3GPP TS 24.501 [64].*"Also, as specified in TS 23.122 sub 3.1 as below (see turquoise text), the UE shall add a PLMN into **the list of "forbidden PLMNs" in the memory** when the PLMN-specific attempt counter for that VPLMN is **less than** the MS implementation specific maximum value."*A VPLMN may be stored in the extension of the "forbidden PLMNs" list if a message with cause value "PLMN not allowed" or "Requested service option not authorized in this PLMN" or "Serving network not authorized" is received by an MS in response to an LR request from that VPLMN, and the following is valid:**- the MS is not configured to use timer T3245, the message is not integrity-protected, the MS maintains a list of PLMN-specific attempt counters and the value of the PLMN-specific attempt counter for that VPLMN is less than an MS implementation specific maximum value as defined in 3GPP TS 24.008 [23], 3GPP TS 24.301 [23A] and 3GPP TS 24.501 [64]*."Based on above statement in TS 23.122, a rejected PLMN can be either stored in **the list of "forbidden PLMNs" in the USIM** or **the list of "forbidden PLMNs" in the memory** but will not be stored twice in both list at the same time.Then come back to above yellow text handling, it may cause a forbidden PLMN will be stored twice, i.e. duplicated in both list of "forbidden PLMNs" in USIM and the list of "forbidden PLMNs" in momory which is unnecessary and waste the UE storage resouces, e.g. in following secenario:1. *The MS is not configured to use timer T3245.*
2. *The UE receives an EMM NAS reject with EMM cause #11 without integrity protection in VPLMN#1.*
3. *The UE maintains a list of PLMN-specific attempt counters and the PLMN-specific attempt counter for VPLMN#1 equals to the MS implementation specific maximum value (e.g. 10).*
4. *As per TS 23.122 sub 3.1, TS 24.301 sub 5.3.7b,* ***the UE adds the VPLMN#1 ID into the list of "forbidden PLMNs" stored in USIM*** *and then* ***as per above yellow text, resets the PLMN-specific attempt counter to zero for VPLMN#1****.*
5. *Hereafter, the user of the UE performs manual PLMN selection to select this PLMN again, requests for registration and rejected with EMM cause #11 without integrity protection.*
6. *As per TS 24.301 sub 5.3.7b, the UE will start T3247 and increments the PLMN-specific attempt counter for VPLMN#1 to 1.*
7. *As the PLMN-specific attempt counter for VPLMN#1 is 1 which is less than the MS implementation specific maximum value (e.g. 10), as per TS 23.122 sub 3.1, TS 24.301 sub 5.3.7b,* ***the UE will add VPLMN#1 into the list of "forbidden PLMNs" stored in momory****.*
8. ***Then it cause the problem that VPLMN#1 is stored twice, i.e. duplicated in both list of "forbidden PLMNs" stored in USIM and the list of "forbidden PLMNs" stored in momory which is unnecessary and waste the UE storage resouces.***

In fact, when a forbidden PLMN was added into the list of "forbidden PLMNs" stored in USIM as per above green text in TS 23.122, it indicates that the UE has tried the registration attempts up to the MS implementation specific maximum value but still rejected. This does mean this PLMN is a real forbidden PLMN, not mounted as DoS attack and it can be safely stored in the list of "forbidden PLMNs" in USIM.Note that in both 24.501 and 24.008, there is no above similar yellow text handling. |
|  |  |
| ***Summary of change:*** | It proposes to remove the UE handling on reset the PLMN-specific attempt counter and the PLMN-specific PS-attempt counter when the PLMN is added to a list of "forbidden PLMNs" in the USIM. |
|  |  |
| ***Consequences if not approved:*** | A forbidden PLMN will be stored twice, i.e. duplicated in both list of "forbidden PLMNs" in USIM and the list of "forbidden PLMNs" in momory which is unnecessary and waste the UE storage resouces |
|  |  |
| ***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 clause 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 clauses 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 maintains the above lists of attempt counters and the event counters, a UE supporting N1 mode, shall store them 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 power saving mode or MICO mode (see 3GPP TS 24.501 [54]).

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 clause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and eKSI;

- if the EMM cause value received is #3, #6 or #8, delete the list of equivalent PLMNs if any;

- 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 clauses 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 clauses 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 clauses 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 clause 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 clause 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 clause5.5.1, 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 clause 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 extension of the "forbidden PLMNs" 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 clause 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], clause 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.

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 UE is switched off or the USIM is removed.

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