**3GPP TSG-CT WG1 Meeting #137-eC1-225191**

**E-Meeting, 18th – 26th August 2022…………………………………………(was C1-224924)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | 5GProtoc18 | | | | |  | ***Date:*** | | | 2022-08-11 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***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 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-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 UE  Some parts of 24.501 already state that network should keep the EMM context unchanged for example below:  “If a SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message fails the integrity check and the UE has only non-emergency PDU sessions established, the AMF shall send the SERVICE REJECT message with 5GMM cause #9 "UE identity cannot be derived by the network" **and keep the 5GMM-context and 5G NAS 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, 5.4.1.3.5, 5.5.1.2.8 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 AMF

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the AMF or forwarded to the 5GSM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST; and

g) DEREGISTRATION ACCEPT;

NOTE 1: The REGISTRATION REQUEST message is sent by the UE without integrity protection, if the registration procedure is initiated due to an inter-system change in 5GMM-IDLE mode and no current 5G NAS security context is available in the UE. The other messages are accepted by the AMF without integrity protection, as in certain situations they are sent by the UE before security can be activated.

NOTE 2: The DEREGISTRATION REQUEST message can be sent by the UE without integrity protection, e.g. if the UE is registered for emergency services and there is no valid 5G NAS security context available, or if due to user interaction a registration 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 registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once a current 5G NAS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF 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 5G NAS security context is not available in the network:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST;

g) DEREGISTRATION ACCEPT;

h) SERVICE REQUEST; and

i) CONTROL PLANE SERVICE REQUEST;

NOTE 3: These messages are processed by the AMF 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 a 5G NAS security context that is no longer available in the network.

If a REGISTRATION REQUEST message for initial registration fails the integrity check and it is not a registration request for emergency services, the AMF shall authenticate the subscriber before processing the registration request any further. Additionally, the AMF shall initiate a security mode control procedure, and include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. If authentication procedure is not successful the AMF shall maintain, if any, the 5GMM-context and 5G NAS security context unchanged. For the case when the registration procedure is for emergency services see subclause 5.5.1.2.3 and subclause 5.4.1.3.5.

If a REGISTRATION REQUEST message for mobility and periodic registration update fails the integrity check and the UE provided EPS NAS message container IE which was successfully verified by the source MME, the AMF may create a mapped 5G NAS security context and initiate a security mode control procedure to take the new mapped 5G NAS security context into use; otherwise if the UE has only a non-emergency PDU session established, the AMF shall initiate a primary authentication and key agreement procedure to create a new native 5G NAS security context. Additionally, the AMF shall initiate a security mode control procedure, and include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. If authentication procedure is not successful the AMF shall maintain, if any, the 5GMM-context and 5G NAS security context unchanged. For the case when the UE has an emergency PDU session see subclause 5.5.1.3.3 and subclause 5.4.1.3.5.

If a DEREGISTRATION REQUEST message fails the integrity check, the AMF shall proceed as follows:

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

- If it is a deregistration request due to switch off, or the AMF does not initiate an authentication procedure for any other reason, the AMF may ignore the deregistration request and remain in state 5GMM-REGISTERED.

NOTE 4: The network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

If a SERVICE REQUEST or CONTROL PLANE SERVICE REQUEST message fails the integrity check and the UE has only non-emergency PDU sessions established, the AMF shall send the SERVICE REJECT message with 5GMM cause #9 "UE identity cannot be derived by the network" and keep the 5GMM-context and 5G NAS security context unchanged. For the case when the UE has an emergency PDU session and integrity check fails, the AMF may skip the authentication procedure even if no 5G NAS security context is available and proceed directly to the execution of the security mode control procedure as specified in subclause 5.4.2. Additionally, the AMF shall include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. After successful completion of the service request procedure, the network shall perform a local release of all non-emergency PDU sessions. The emergency PDU sessions shall not be released.

Once the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF 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 AMF 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 \*\*\*\*\*

##### 5.4.1.3.5 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 5G-GUTI was used; or

- if the SUCI was used.

If the 5G-GUTI was used, the network should initiate an identification procedure to retrieve SUCI from the UE and restart the 5G AKA based primary authentication and key agreement procedure with the received SUCI.

If the SUCI was used for identification in the initial NAS message or in a restarted 5G AKA based primary authentication and key agreement procedure, or the network decides not to initiate the identification procedure to retrieve SUCI from the UE after an unsuccessful 5G AKA based primary authentication and key agreement procedure, the network should send an AUTHENTICATION REJECT message to the UE. The network shall maintain, if any, the 5GMM-context and 5G NAS security context of the UE unchanged.

Upon receipt of an AUTHENTICATION REJECT message,

1) if the AUTHENTICATION REJECT message has been successfully integrity checked by the NAS:

the UE shall set the update status to 5U3 ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI.

In case of PLMN, the USIM shall be considered invalid until switching off the UE or the UICC containing the USIM is removed.

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE does not support access to an SNPN using credentials from a credentials holder, the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid until the UE is switched off or the entry is updated. Additionally, the UE shall consider the USIM as invalid for the current SNPN until switching off or the UICC containing the USIM is removed.

In case of SNPN, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN and the UE supports access to an SNPN using credentials from a credentials holder, the UE shall consider the selected entry of the "list of subscriber data" as invalid for 3GPP access until the UE is switched off or the entry is updated. Additionally, the UE shall consider the USIM as invalid for the entry until switching off or the UICC containing the USIM is removed.

In case of SNPN, if the UE is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN, the UE shall store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5]; and

- if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall set:

i) the counter for "SIM/USIM considered invalid for GPRS services" events, the counter for "USIM considered invalid for 5GS services over non-3GPP access" events, and the counter for "SIM/USIM considered invalid for non-GPRS services" events if maintained by the UE, in case of PLMN; or

ii) the counter for "the entry for the current SNPN considered invalid for 3GPP access" events and the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN;

to UE implementation-specific maximum value.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall set the SNPN-specific attempt counter for the current SNPN to the UE implementation-specific maximum value; and

- if the UE is operating in single-registration mode, the UE shall handle EMM parameters, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the authentication procedure is not accepted by the network. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed; and

2) if the AUTHENTICATION REJECT message is received without integrity protection and if timer T3516 or T3520 is running, the UE shall start timer T3247 with a random value uniformly drawn from the range between 30 minutes and 60 minutes, if the timer is not running (see subclause 5.3.20).

Additionally, if the UE is neither registered for onboarding services in SNPN nor performing initial registration for onboarding services in SNPN, the UE shall:

a) if the AUTHENTICATION REJECT message is received over 3GPP access, and the counter for "SIM/USIM considered invalid for GPRS services" events in case of PLMN or the counter for "the entry for the current SNPN considered invalid for 3GPP access" events in case of SNPN has a value less than a UE implementation-specific maximum value, proceed as specified in subclause 5.3.20, list item 1)-a) of subclause 5.3.20.2 (if the UE is not operating in SNPN access operation mode) or list item a)-1) of subclause 5.3.20.3 (if the UE is operating in SNPN access operation mode) for the case that the 5GMM cause value received is #3;

b) if the AUTHENTICATION REJECT message is received over non-3GPP access, and the counter for "USIM considered invalid for 5GS services over non-3GPP access" events in case of PLMN or the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events in case of SNPN has a value less than a UE implementation-specific maximum value, proceed as specified in subclause 5.3.20, list item 1)-b) of subclause 5.3.20.2 (if the UE is not operating in SNPN access operation mode) or list item a)-2) of subclause 5.3.20.3 (if the UE is operating in SNPN access operation mode) for the case that the 5GMM cause value received is #3.

c) otherwise:

i) if the AUTHENTICATION REJECT message is received over 3GPP access:

- The UE shall set the update status for 3GPP access to 5U3 ROAMING NOT ALLOWED, delete for 3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI.

- In case of PLMN, the UE shall consider the USIM as invalid for 5GS services via 3GPP access and non-EPS service until switching off the UE or the UICC containing the USIM is removed.

In case of SNPN, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid for 3GPP access until the UE is switched off or the entry is updated. Additionally, the UE shall consider the USIM as invalid for the current SNPN via 3GPP access until switching off or the UICC containing the USIM is removed.

- The UE shall set:

- the counter for "SIM/USIM considered invalid for GPRS services" events and the counter for "SIM/USIM considered invalid for non-GPRS services" events if maintained by the UE, in case of PLMN; or

- the counter for "the entry for the current SNPN considered invalid for 3GPP access" events in case of SNPN;

to UE implementation-specific maximum value.

- If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the authentication procedure is not accepted by the network. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed; and

ii) if the AUTHENTICATION REJECT message is received over non-3GPP access:

- the UE shall set the update status for non-3GPP access to 5U3 ROAMING NOT ALLOWED, delete for non-3GPP access only the stored 5G-GUTI, TAI list, last visited registered TAI and ngKSI;

- in case of PLMN, the UE shall consider the USIM as invalid for 5GS services via non-3GPP access until switching off the UE or the UICC containing the USIM is removed.

In case of SNPN, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN as invalid for non-3GPP access until the UE is switched off or the entry is updated. Additionally, the UE shall consider the USIM as invalid for the current SNPN and for non-3GPP access until switching off or the UICC containing the USIM is removed; and

- the UE shall set:

- the counter for "USIM considered invalid for 5GS services over non-3GPP access" events to UE implementation-specific maximum value in case of PLMN; or

- the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events to UE implementation-specific maximum value in case of SNPN.

If the UE is registered for onboarding services in SNPN or performing initial registration for onboarding services in SNPN, the UE shall:

1) if the SNPN-specific attempt counter for the SNPN sending the AUTHENTICATION REJECT message has a value less than a UE implementation-specific maximum value, increment the SNPN-specific attempt counter for the SNPN; or

2) otherwise, the UE shall set the update status to 5U3.ROAMING NOT ALLOWED, delete the stored 5G-GUTI, TAI list, last visited registered TAI, and ngKSI, store the SNPN identity in the "permanently forbidden SNPNs" list for onboarding services, enter state 5GMM-DEREGISTERED.PLMN-SEARCH, and perform an SNPN selection or an SNPN selection for onboarding services according to 3GPP TS 23.122 [5].

If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any 5GMM signalling procedure, stop any of the timers T3510, T3516, T3517, T3519, T3520 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

Depending on local requirements or operator preference for emergency services, if the UE initiates a registration procedure with 5GS registration type IE set to "emergency registration" and the AMF is configured to allow emergency registration without user identity, the AMF needs not follow the procedures specified for the authentication failure in the present subclause. The AMF may continue a current 5GMM specific procedure.

\*\*\*\*\*Next change \*\*\*\*\*

##### 5.5.1.2.8 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 REGISTRATION COMPLETE message has been received from the UE and timer T3550 is running, the AMF shall locally abort the registration procedure for initial registration, enter state 5GMM-REGISTERED and shall not resend the REGISTRATION ACCEPT message. If a new 5G-GUTI was assigned to the UE in the registration procedure for initial registration, the AMF shall consider both the old and the new 5G-GUTI as valid until the old 5G-GUTI can be considered as invalid by the AMF or the 5GMM context which has been marked as deregistered in the AMF is released. If the old 5G-GUTI was allocated by an AMF other than the current AMF, the current AMF does not need to retain the old 5G-GUTI. During this period the network may use the identification procedure followed by a generic UE configuration update procedure if the old 5G-GUTI is used by the UE in a subsequent message.

b) Protocol error

If the REGISTRATION REQUEST message is received with a protocol error, the AMF shall return a REGISTRATION REJECT message with one of the following 5GMM cause values:

#96 invalid mandatory information;

#99 information element non-existent or not implemented;

#100 conditional IE error; or

#111 protocol error, unspecified.

c) T3550 time-out

On the first expiry of the timer, the AMF shall retransmit the REGISTRATION ACCEPT message and shall reset and restart timer T3550.

This retransmission is repeated four times, i.e. on the fifth expiry of timer T3550, the registration procedure for initial registration shall be aborted and the AMF enters state 5GMM-REGISTERED. If a new 5G-GUTI was allocated in the REGISTRATION ACCEPT message, the AMF shall consider both the old and the new 5G-GUTIs as valid until the old 5G-GUTI can be considered as invalid by the AMF or the 5GMM context which has been marked as de-registered in the AMF is released. If the old 5G-GUTI was allocated by an AMF other than the current AMF, the current AMF does not need to retain the old 5G-GUTI. During this period, if the old 5G-GUTI is used by the UE in a subsequent message, the AMF acts as specified for case a) above.

d) REGISTRATION REQUEST message received after the REGISTRATION ACCEPT message has been sent and before the REGISTRATION COMPLETE message is received, if the REGISTRATION COMPLETE message is expected.

1) If one or more of the information elements in the REGISTRATION REQUEST message differ from the ones received within the previous REGISTRATION REQUEST message, the previously initiated the registration procedure for initial registration shall be aborted if the REGISTRATION COMPLETE message has not been received and the new registration procedure for initial registration shall be progressed; or

2) if the information elements do not differ, then the REGISTRATION ACCEPT message shall be resent and the timer T3550 shall be restarted. In that case, the retransmission counter related to T3550 is not incremented.

e) More than one REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" received and no REGISTRATION ACCEPT message or REGISTRATION REJECT message has been sent.

1) If one or more of the information elements in the REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" differs from the ones received within the previous REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration", the previously initiated the registration procedure for initial registration shall be aborted and the new the registration procedure for initial registration shall be executed;

2) if the information elements do not differ, then the network shall continue with the previous the registration procedure for initial registration and shall ignore the second REGISTRATION REQUEST message.

f) REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" received in state 5GMM-REGISTERED.

If a REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" is received in state 5GMM-REGISTERED the network may initiate the 5GMM common procedures; if it turned out that the REGISTRATION REQUEST message was sent by a genuine UE that has already been registered, the 5GMM context, if any, are deleted and the new REGISTRATION REQUEST is progressed, otherwise if network considers REGISTRATION REQUEST message was not sent by a genuine UE based on authentication procedure the network shall maintain the 5GMM-context, if any, unchanged.

NOTE 1: The network can determine that the UE is genuine by executing the authentication procedure as described in subclause 5.4.1.

g) REGISTRATION REQUEST message with 5GS registration type IE set to "mobility registration updating" or "periodic registration updating" received before REGISTRATION COMPLETE message, if the REGISTRATION COMPLETE message is expected.

Timer T3550 shall be stopped. The allocated 5G-GUTI in the registration procedure for initial registration shall be considered as valid and the registration procedure for mobility and periodic update shall be progressed as described in subclause 5.5.1.3.

h) DEREGISTRATION REQUEST message received before REGISTRATION COMPLETE message, if the REGISTRATION COMPLETE message is expected.

The AMF shall abort the registration procedure for initial registration and shall progress the de-registration procedure as described in subclause 5.5.2.2.

i) UE security capabilities invalid or unacceptable

If the REGISTRATION REQUEST message is received with invalid or unacceptable UE security capabilities (e.g. no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported, etc.), the AMF shall return a REGISTRATION REJECT message.

NOTE 2: 5GMM cause value to be used in REGISTRATION REJECT message is up to the network implementation.

j) Based on operator policy, if the initial registration request from a UE not supporting CAG is rejected due to CAG restrictions, the network shall reject the initial registration with a 5GMM cause value other than the 5GMM cause #76 (Not authorized for this CAG or authorized for CAG cells only).

NOTE 3: 5GMM cause #7 (5GS services not allowed), 5GMM cause #11 (PLMN not allowed), 5GMM cause #27 (N1 mode not allowed), 5GMM cause #73 (Serving network not authorized) can be used depending on the subscription of the UE and whether the UE roams or not.

\*\*\*\*\*End change \*\*\*\*\*