**3GPP TSG-CT WG1 Meeting #133e-bisC1-22xxxx**

**E-meeting, 17-21 January 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3918** | **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:***  | Handling of a non-integrity protected AUTHENTICATION REJECT message received from an ON-SNPN |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2022-01-17 |
|  |  |  |  |  |
| ***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:*** | The following EN requires resolution.Editor's note: Handling of a non-integrity protected AUTHENTICATION REJECT message by a UE which is registered for onboarding services in SNPN or is performing initial registration for onboarding services in SNPN is FFS. |
|  |  |
| ***Summary of change:*** | The EN is resolved. The proposed UE behavior is to enter state 5GMM-DEREGISTERED.PLMN-SEARCH and perform an SNPN selection for onboarding services according to 3GPP TS 23.122 if the counter reaches the maximum value. |
|  |  |
| ***Consequences if not approved:*** | The EN remains. |
|  |  |
| ***Clauses affected:*** | 5.4.1.2.2.11, 5.4.1.2.3.1, 5.4.1.2.3A.1, 5.4.1.3.5 |
|  |  |
|  | **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:*** |  |

5.4.1.2.2.11 UE handling EAP-failure message

Upon receiving an EAP-failure message, the UE shall delete the partial native 5G NAS security context and shall delete the new KAUSF and the new KSEAF, if any were created as described in subclause 5.4.1.2.2.3.

The UE shall consider the procedure complete.

If the EAP-failure message is received in 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 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 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 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;

- 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; 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, 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 invalid for non-EPS service until switching off the UE or the UICC containing the USIM is removed.

 In case of SNPN, if the UE does not support access to an SNPN using credentials from a credentials holder, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN 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 current SNPN via 3GPP access until switching off or the UICC containing the USIM is removed.

 In case of SNPN, if 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 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:

a) 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

b) 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, T3517, T3519 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

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

5.4.1.2.3.1 General

The UE may support acting as EAP-TLS peer as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP-TLS server as specified in 3GPP TS 33.501 [24]. The AAA server of the CH may support acting as EAP server of such EAP method as specified in 3GPP TS 23.501 [8].

Editor's note: (WI:eNPN, CR:3675): it is FFS how the UE determines that the credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server.

The EAP-TLS enables mutual authentication of the UE and the network.

When initiating an EAP based primary authentication and key agreement procedure using EAP-TLS, the network shall select an ngKSI value. If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall select a different ngKSI value. The network shall send the selected ngKSI value to the UE along with each EAP message. The network shall send the ABBA value as described in subclause 9.11.3.10 to the UE along with the EAP-request message and EAP-success message.

When the EAP based primary authentication and key agreement procedure uses EAP-TLS:

a) if the UE operates in SNPN access operation mode and credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then the ME shall generate MSK as described in 3GPP TS 33.501 [24] otherwise the ME shall generate EMSKas described in 3GPP TS 33.501 [24];

b) if the AUSF acts as the EAP-TLS server, the AUSF shall generate EMSKas described in 3GPP TS 33.501 [24]; and

c) if the AAA server of the CH acts as the EAP-TLS server, the AAA server of the CH shall generate MSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of:

a) MSK and credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server, the ME may generate a new KAUSF from the MSK; or

b) EMSK and credentials in the selected entry of the "list of configuration data" are not from a CH with the AAA server or the UE does not operate in SNPN access operation mode, the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request message in subclause 5.4.1.2.4.2, in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context.

NOTE 1: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

The ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

When the AUSF acts as the EAP-TLS server and handling of an EAP response message results into generation of EMSK, the AUSF shall generate the KAUSF from the EMSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 2: When the AAA server of the CH acts as the EAP-TLS server, the AAA server of the CH provides (via the NSSAAF) the MSK to the AUSF. Upon reception of the MSK, the AUSF generates the KAUSF from the MSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 3: The AUSF provides the KSEAF to the SEAF. Upon reception of the KSEAF, the SEAF generates the KAMF based on the ABBA and the KSEAF as described in 3GPP TS 33.501 [24], and provides ngKSI and the KAMF to the AMF. Upon reception of the ngKSI and the KAMF, the AMF creates a partial native 5G NAS security context identified by the ngKSI, and stores the KAMF in the created partial native 5G NAS security context.

If the UE does not accept the server certificate of the network, the UE shall start timer T3520 when the AUTHENTICATION RESPONSE message containing the EAP-response message is sent. Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon receiving an AUTHENTICATION REQUEST message with the EAP message IE containing an EAP-request message from the network, the UE shall stop timer T3520, if running, and then process the EAP-request message as normally.

If the network does not accept the client certificate of the UE, the network handling 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 transport the EAP-failure message in the AUTHENTICATION RESULT message of the EAP result message transport procedure, initiate an identification procedure to retrieve SUCI from the UE and restart the EAP 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 EAP 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 the EAP based primary authentication and key agreement procedure, the network should transport the EAP-failure message in an AUTHENTICATION REJECT message of the EAP result message transport procedure.

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 transporting the EAP-failure message in the AUTHENTICATION REJECT message of the EAP result message transport procedure in the present subclause. The AMF may include the EAP-failure message in a response of the current 5GMM specific procedure or in the AUTHENTICATION RESULT of the EAP result message transport procedure.

If the EAP-failure message is received in an AUTHENTICATION REJECT message:

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

1) 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;

 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 until the UE is switched off or the entry is updated.

 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 the specific access type for which the message was received;

Editor's note: It is FFS how the UE operates after storing the SNPN identity in the "permanently forbidden SNPNs" list for the specific access type for which the message was received.

2) 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;

NOTE 4: The term "non-3GPP access" used in the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events, is used to express access to SNPN services via a PLMN.

 to UE implementation-specific maximum value; and

3) 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

b) if the AUTHENTICATION REJECT message is received without integrity protection, 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:

1) 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 SNPN enabled or 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;

2) 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; or

3) otherwise:

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

A) 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 invalid for non-EPS service until switching off the UE or the UICC containing the USIM is removed.

 In case of SNPN, if the UE does not support access to an SNPN using credentials from a credentials holder, the UE shall consider the entry of the "list of subscriber data" with the SNPN identity of the current SNPN as invalid for 3GPP access until the UE is switched off or the entry is updated;

 In case of SNPN, if 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;

B) 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; and

C) 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:

A) 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 USIM shall be considered 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 shall be considered invalid for non-3GPP access until the UE is switched off or the entry is updated; and

B) the UE shall set 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 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:

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, T3517, T3519 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

Upon receiving an EAP-success message, the ME shall:

a) delete the valid KAUSF and the valid KSEAF, if any;

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK or MSK as described above:

1) if the UE operates in SNPN access operation mode and credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the new KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) consider the new KAUSF to be the valid KAUSF, and the new KSEAF to be the valid KSEAF, reset the SOR counter and the UE parameter update counter to zero, store the valid KAUSF, the valid KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and use the valid KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received.

The UE shall consider the procedure complete.

Upon receiving an EAP-failure message, the UE shall delete the partial native 5G NAS security context and shall delete the new KAUSF and the new KSEAF, if any were created when handling the EAP-request message which resulted into generation of EMSK or MSK as described above.

The UE shall consider the procedure complete.

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

5.4.1.2.3A.1 General

his subclause applies when an EAP method:

a) supporting mutual authentication;

b) supporting EMSK or MSK generation; and

c) other than EAP-AKA' and EAP-TLS;

is used for primary authentication and key agreement in an SNPN.

The UE may support acting as EAP peer of such EAP method as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP server of such EAP method as specified in 3GPP TS 33.501 [24]. The AAA server of the CH may support acting as EAP server of such EAP method as specified in 3GPP TS 23.501 [8].

Editor's note: (WI:eNPN, CR:3675): it is FFS how the UE determines that the credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server.

When initiating an EAP based primary authentication and key agreement procedure using such EAP method, the network shall select an ngKSI value. If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall select a different ngKSI value. The network shall send the selected ngKSI value to the UE along with each EAP message. The network shall send the ABBA value as described in subclause 9.11.3.10 to the UE along with the EAP-request message and EAP-success message.

When the EAP based primary authentication and key agreement procedure uses such EAP method:

a) if credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then the ME shall generate MSK as described in 3GPP TS 33.501 [24] otherwise the ME shall generate EMSKas described in 3GPP TS 33.501 [24];

b) if the AUSF acts as the EAP server, the AUSF shall generate EMSK as described in 3GPP TS 33.501 [24]; and

c) if the AAA server of the CH acts as the EAP server, the AAA server of the CH shall generate MSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of:

a) MSK and credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then the ME may generate a new KAUSF from the MSK; or

b) EMSK and credentials in the selected entry of the "list of configuration data" are not from a CH with the AAA server then the ME may generate a new KAUSF from the EMSK.

If the ME generates a new KAUSF, the ME shall generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the new KSEAF as described in 3GPP TS 33.501 [24], and create a partial native 5G NAS security context identified by the ngKSI value received together with the EAP-request message in subclause 5.4.1.2.4.2, in the volatile memory of the ME. If the KAMF and the partial native 5G NAS security context are created, the ME shall store the KAMF in the created partial native 5G NAS security context.

NOTE 1: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

The ME shall not use the new KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received, until receipt of an EAP-success message.

When the AUSF acts as the EAP server and handling of an EAP response message results into generation of EMSK, the AUSF shall generate the KAUSF from the EMSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 2: When the AAA server of the CH acts as the EAP server and handling of an EAP response message results into generation of MSK, the AAA server of the CH provides (via the NSSAAF) the MSK to the AUSF. Upon reception of the MSK, the AUSF generates the KAUSF from the MSK, and the KSEAF from the KAUSF as described in 3GPP TS 33.501 [24].

NOTE 3: The AUSF provides the KSEAF to the SEAF. Upon reception of the KSEAF, the SEAF generates the KAMF based on the ABBA and the KSEAF as described in 3GPP TS 33.501 [24], and provides ngKSI and the KAMF to the AMF. Upon reception of the ngKSI and the KAMF, the AMF creates a partial native 5G NAS security context identified by the ngKSI, and stores the KAMF in the created partial native 5G NAS security context.

If the UE fails to authenticate the network, the UE shall start timer T3520 when the AUTHENTICATION RESPONSE message containing the EAP-response message is sent. Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon receiving an AUTHENTICATION REQUEST message with the EAP message IE containing an EAP-request message from the network, the UE shall stop timer T3520, if running, and then process the EAP-request message as normally.

If the network fails to authenticate the UE, the network handling 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 transport the EAP-failure message in the AUTHENTICATION RESULT message of the EAP result message transport procedure, initiate an identification procedure to retrieve SUCI from the UE and restart the EAP 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 EAP 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 the EAP based primary authentication and key agreement procedure, the network should transport the EAP-failure message in an AUTHENTICATION REJECT message of the EAP result message transport procedure.

If the EAP-failure message is received in an AUTHENTICATION REJECT message:

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

1) 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 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;

 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 until the UE is switched off or the entry is updated.

 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 the specific access type for which the message was received; and

Editor's note: It is FFS how the UE operates after storing the SNPN identity in the "permanently forbidden SNPNs" list for the specific access type for which the message was received.

2) the UE shall set 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; and

NOTE 4: The term "non-3GPP access" used in the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events, is used to express access to SNPN services via a PLMN.

b) if the AUTHENTICATION REJECT message is received without integrity protection, 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:

1) if the AUTHENTICATION REJECT message is received over 3GPP access, and the counter for "the entry for the current SNPN considered invalid for 3GPP access" events has a value less than a UE implementation-specific maximum value, proceed as specified in list item a) 1) of subclause 5.3.20.3 for the case that the 5GMM cause value received is #3;

2) if the AUTHENTICATION REJECT message is received over non-3GPP access, and the counter for "the entry for the current SNPN considered invalid for non-3GPP access" events has a value less than a UE implementation-specific maximum value, proceed as specified in list item a)-2) of subclause 5.3.20.3 for the case that the 5GMM cause value received is #3; or

3) 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 SNPN, if 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 for 3GPP access until the UE is switched off or the entry is updated;

 In case of SNPN, if 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 until the UE is switched off or the entry is updated; and

- the UE shall set the counter for "the entry for the current SNPN considered invalid for 3GPP access" events to UE implementation-specific maximum value; 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. The entry of the "list of subscriber data" with the SNPN identity of the current SNPN shall be considered invalid for non-3GPP access until the UE is switched off or the entry is updated; and

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

NOTE 5: The AUTHENTICATION REJECT message "received over non-3GPP access" in this subclause refers to an AUTHENTICATION REJECT message received via a PLMN when the UE attempts to access SNPN services via a PLMN.

 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, T3517, T3519 or T3521 (if they were running), enter state 5GMM-DEREGISTERED and delete any stored SUCI.

Upon receiving an EAP-success message, the ME shall:

a) delete the valid KAUSF and the valid KSEAF, if any;

b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK as described above:

1) if credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;

2) generate a new KSEAF from the new KAUSF, and the KAMF from the ABBA that was received with the EAP-success message, and the KSEAF as described in 3GPP TS 33.501 [24];

3) create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME; and

4) store the KAMF in the created partial native 5G NAS security context; and

c) consider the new KAUSF to be the valid KAUSF, and the new KSEAF to be the valid KSEAF, reset the SOR counter and the UE parameter update counter to zero, store the valid KAUSF, the valid KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and use the valid KAUSF in the verification of SOR transparent container and UE parameters update transparent container, if any are received.

The UE shall consider the procedure complete.

Upon receiving an EAP-failure message, the UE shall delete the partial native 5G NAS security context and shall delete the new KAUSF and the new KSEAF, if any were created when handling the EAP-request message which resulted into generation of EMSK or MSK as described above.

The UE shall consider the procedure complete.

\*\*\*\*\* 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.

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 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 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;

- 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; 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.

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.