**3GPP TSG-CT WG1 Meeting #128-eC1-21XXXX**

**Electronic meeting, 25 February – 5 March 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **3065** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Marking KAUSF as valid | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2021-02-10 |
|  |  | | | |  | |  | | |  |
| ***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 can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) ... Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As per requested in the SA3 LS C1-210531/S3-210706 as below:  "*SA3 is considering a solution, where only after identifying that the primary (re)authentication is successful in the network side, the UE shall store the KAUSF, SOR counter and UE parameter update counter on the USIM (or in the non-volatile memory of the ME, if no corresponding file is present on the USIM). The UE identifies that the primary (re)authentication is successful in the network side, upon receiving a valid NAS Security Mode Command message.*  *The solution under consideration mandates performing NAS SMC procedure, after the successful run of primary authentication. Running of the NAS SMC procedure after primary authentication as soon as possible is essential to keep the stored KAUSF aligned between the UE and home network. On this new mandatory requirement under consideration, SA3 would like to have feedback from CT1 and CT4, on the feasibility to perform NAS SMC procedure immediately after successful run of primary authentication.* "  Note that though as indicated in the original CT1 LS C1-207764, the open issue is only for 5G AKA procedure, but SA3 LS does not mention which specific AKA procedure the above SA3 requirement applies. Hence, by default it is applied to both EAP AKA-based and 5G AKA-based procedures. This could provide a simpler and consistent network handling on confirming the successful AKA to the UE.  At the UE side, once confimed by the SMC message that the AKA procedure was successfully performed at the network side, then it can delete the old valid KAUSF if any,store the newly generated KAUSF in to non-volatile memory of ME or USIM and consider the stored KAUSF as valid.  Note that as indicated in SA3 LS, it is still FFS about the storage of KSEAF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It proposes:   1. For EAP AKA, the UE shall consider the stored KAUSF as valid when it receives a SECURITY MODE COMMAND message including an EAP-success message. 2. For 5G AKA, the UE shall consider the stored KAUSF as valid when it receives a SECURITY MODE COMMAND message. 3. For both EAP AKA and 5G AKA, when the UE stores the newly generated KAUSF, it also needs to delete the old valid KAUSF if any. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UE handling on when to treat the newly generated KAUSF during a successful primary authentication and key agreement procedure as valid is unclear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.1.2.2.8, 5.4.1.2.3.1, 5.4.1.2.3A.1, 5.4.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

###### 5.4.1.2.2.8 UE handling EAP-success message

Upon receiving an EAP-success message, if the ME has not generated a partial native 5G NAS security context as described in subclause 5.4.1.2.2.3, the ME shall:

a) generate the KAUSF from the EMSK, the KSEAF from the 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];

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

c) store the KAMF in the created partial native 5G NAS security context.

The ME shall reset the SOR counter and the UE parameter update counter to zero, delete the old valid KAUSF if any, store the newly generated KAUSF, KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and consider the stored KAUSF as valid.

The UE shall consider the procedure complete.

\* \* \* 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 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, the ME and the AUSF shall generate EMSKas described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of EMSK, the ME may generate the KAUSF from the EMSK, the KSEAF from the KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the 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.

When 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 1: 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, 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;

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 2: 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, 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 mode) or list item a) 1) of subclause 5.3.20.3 (if the UE is operating in SNPN access 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 mode) or list item a)-2) of subclause 5.3.20.3 (if the UE is operating in SNPN access 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, 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;

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 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, if the ME has not generated a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK as described above , the ME shall generate the KAUSF from the EMSK, the KSEAF from the 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], shall create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME, and shall store the KAMF in the created partial native 5G NAS security context.

Additionally, upon receiving the EAP-success message, the ME shall reset the SOR counter and the UE parameter update counter to zero, delete the old valid KAUSF if any, store the newly generated KAUSF, KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and consider the stored KAUSF as valid.

The UE shall consider the procedure complete.

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

The UE shall consider the procedure complete.

\* \* \* Next Change \* \* \* \*

###### 5.4.1.2.3A.1 General

This subclause applies when an EAP method:

a) supporting mutual authentication;

b) supporting EMSK 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].

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, the ME and the AUSF shall generate EMSK as described in 3GPP TS 33.501 [24].

When handling of an EAP-request message results into generation of EMSK, the ME may generate the KAUSF from the EMSK, the KSEAF from the KAUSF, and the KAMF from the ABBA received together with the EAP-request message, and the 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.

When 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 1: 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. 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; and

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 2: 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, 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. 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; 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 3: 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 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, if the ME has not generated a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK as described above , the ME shall generate the KAUSF from the EMSK, the KSEAF from the 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], shall create a partial native 5G NAS security context identified by the ngKSI value in the volatile memory of the ME, and shall store the KAMF in the created partial native 5G NAS security context.

Additionally, upon receiving the EAP-success message, the ME shall reset the SOR counter and the UE parameter update counter to zero, delete the old valid KAUSF if any, store the newly generated KAUSF, KSEAF, the SOR counter and the UE parameter update counter as specified in annex C, and consider the stored KAUSF as valid.

The UE shall consider the procedure complete.

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

The UE shall consider the procedure complete.

\* \* \* Next Change \* \* \* \*

#### 5.4.2.3 NAS security mode command accepted by the UE

Upon receipt of the SECURITY MODE COMMAND message, the UE shall check whether the security mode command can be accepted or not. This is done by performing the integrity check of the message, and by checking that the received Replayed UE security capabilities IE has not been altered compared to the latest values that the UE sent to the network.

When the SECURITY MODE COMMAND message includes an EAP-success message the UE handles the EAP-success message and the ABBA as described in subclause 5.4.1.2.2.8, 5.4.1.2.3.1, 5.4.1.2.3A.1 and 5.4.1.2.3B.1.

When the SECURITY MODE COMMAND message is received following a successful 5G AKA based primary authentication and key agreement procedure, the ngKSI included in the SECURITY MODE COMMAND message is that of the new partial native 5G NAS security context, and the integrity check of the SECURITY MODE COMMAND message is successful, the ME shall reset the SOR counter and the UE parameter update counter to zero, delete the old valid KAUSF if any, store the newly generated KAUSF, the SOR counter and the UE parameter update counter as specified in annex C, and consider the stored KAUSF as valid.

Editor's note: It is FFS for when to store the KSEAF and consider it as valid when the SECURITY MODE COMMAND message is received following a successful 5G AKA based primary authentication and key agreement procedure.

If:

a) the UE is registered for emergency services, performing initial registration for emergency services or establishing an emergency PDU session;

b) the W-AGF acts on behalf of the FN-RG; or

c) the W-AGF acts on behalf of the N5GC device,

and the SECURITY MODE COMMAND message is received with ngKSI value "000" and 5G-IA0 and 5G-EA0 as selected 5G NAS security algorithms, the UE shall locally derive and take in use 5G NAS security context. The UE shall delete existing current 5G NAS security context.

The UE shall accept a SECURITY MODE COMMAND message indicating the "null integrity protection algorithm" 5G-IA0 as the selected 5G NAS integrity algorithm only if the message is received when the UE is registered for emergency services, performing initial registration for emergency services or establishing an emergency PDU session or when the W-AGF acts on behalf of the FN-RG, or when the W-AGF acts on behalf of the N5GC device.

If the type of security context flag included in the SECURITY MODE COMMAND message is set to "native security context" and if the ngKSI matches a valid non-current native 5G NAS security context held in the UE while the UE has a mapped 5G NAS security context as the current 5G NAS security context, the UE shall take the non-current native 5G NAS security context into use which then becomes the current native 5G NAS security context and delete the mapped 5G NAS security context.

The UE shall ignore the Replayed S1 UE security capabilities IE if this IE is included in the SECURITY MODE COMMAND message.

If the SECURITY MODE COMMAND message can be accepted, the UE shall take the 5G NAS security context indicated in the message into use. The UE shall in addition reset the uplink NAS COUNT counter if:

a) the SECURITY MODE COMMAND message is received in order to take a 5G NAS security context into use created after a successful execution of the 5G AKA based primary authentication and key agreement procedure or the EAP based primary authentication and key agreement procedure; or

b) the SECURITY MODE COMMAND message received includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE the ngKSI does not match the current 5G NAS security context, if it is a mapped 5G NAS security context.

If the SECURITY MODE COMMAND message can be accepted and a new 5G NAS security context is taken into use and SECURITY MODE COMMAND message does not indicate the "null integrity protection algorithm" 5G-IA0 as the selected NAS integrity algorithm, the UE shall:

- if the SECURITY MODE COMMAND message has been successfully integrity checked using an estimated downlink NAS COUNT equal to 0, then the UE shall set the downlink NAS COUNT of this new 5G NAS security context to 0;

- otherwise the UE shall set the downlink NAS COUNT of this new 5G NAS security context to the downlink NAS COUNT that has been used for the successful integrity checking of the SECURITY MODE COMMAND message.

If the SECURITY MODE COMMAND message includes the horizontal derivation parameter indicating "KAMF derivation is required", the UE shall derive a new K'AMF, as specified in 3GPP TS 33.501 [24] for KAMF to K'AMF derivation in mobility, and set both uplink and downlink NAS COUNTs to zero. When the new 5G NAS security context is taken into use for current access and the UE is registered with the same PLMN over the 3GPP access and the non-3GPP access:

a) the UE is in 5GMM-IDLE mode over the non-current access, the AMF and the UE shall activate the new 5G NAS security context over the non-current access as described in 3GPP TS 33.501 [24]. The AMF and the UE shall set the downlink NAS COUNT and uplink NAS COUNT to zero for the non-current access; or

b) the UE is in 5GMM-CONNECTED mode over the non-current access, the AMF shall send the SECURITY MODE COMMAND message over the non-current access to activate the new 5G NAS security context that was activated over the current access as described in 3GPP TS 33.501 [24]. The AMF shall include the same ngKSI in the SECURITY MODE COMMAND message to identify the new 5G NAS security context.

If the SECURITY MODE COMMAND message includes the horizontal derivation parameter indicating "KAMF derivation is not required" or the Additional 5G security information IE is not included in the message, the UE is registered with the same PLMN over the 3GPP access and non-3GPP access, then after the completion of a security mode control procedure over the current access:

a) the UE is in 5GMM-IDLE mode over the non-current access, the AMF and the UE shall activate the new 5G NAS security context for the non-current access. If a primary authentication and key agreement procedure was completed before the security mode control procedure, the AMF and the UE shall set the downlink NAS COUNT and uplink NAS COUNT to zero for the non-current access, otherwise the downlink NAS COUNT and uplink NAS COUNT for the non-3GPP access are not changed; or

b) the UE is in 5GMM-CONNECTED mode over the non-current access, the AMF shall send the SECURITY MODE COMMAND message over the non-current access to activate the new 5G NAS security context that was activated over the current access as described in 3GPP TS 33.501 [24]. The AMF shall include the same ngKSI in the SECURITY MODE COMMAND message to identify the new 5G NAS security context.

If the SECURITY MODE COMMAND message can be accepted, the UE shall send a SECURITY MODE COMPLETE message integrity protected with the selected 5GS integrity algorithm and the 5G NAS integrity key based on the KAMF or mapped K'AMF if the type of security context flag is set to "mapped security context" indicated by the ngKSI. When the SECURITY MODE COMMAND message includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE, then the UE shall check whether the SECURITY MODE COMMAND message indicates the ngKSI of the current 5GS security context, if it is a mapped 5G NAS security context, in order not to re-generate the K'AMF.

Furthermore, if the SECURITY MODE COMMAND message can be accepted, the UE shall cipher the SECURITY MODE COMPLETE message with the selected 5GS ciphering algorithm and the 5GS NAS ciphering key based on the KAMF or mapped K'AMF indicated by the ngKSI. The UE shall set the security header type of the message to "integrity protected and ciphered with new 5G NAS security context".

From this time onward the UE shall cipher and integrity protect all NAS signalling messages with the selected 5GS integrity and ciphering algorithms.

If the AMF indicated in the SECURITY MODE COMMAND message that the IMEISV is requested and:

a) if the UE:

1) supports at least one 3GPP access technology, the UE shall include its IMEISV in the IMEISV IE of the SECURITY MODE COMPLETE message; or

2) does not support any 3GPP access technology (i.e. NG-RAN, E-UTRAN, UTRAN or GERAN) and supports NAS over untrusted or trusted non-3GPP access, the UE shall include its EUI-64 in the non-IMEISV PEI IE of the SECURITY MODE COMPLETE message; or

b) if the 5G-RG contains neither an IMEISV nor an IMEI or when the W-AGF acts on behalf of the FN-RG (or on behalf of the N5GC device), the 5G-RG or the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) shall include the MAC address and the MAC address usage restriction indication determined as specified in subclause 5.3.2 in the non-IMEISV PEI IE in the SECURITY MODE COMPLETE message.

If during an ongoing registration procedure or service request procedure, the UE receives a SECURITY MODE COMMAND message which includes the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested", the UE shall include the entire unciphered REGISTRATION REQUEST message or SERVICE REQUEST message or CONTROL PLANE SERVICE REQUEST message, which the UE had previously included in the NAS message container IE of the initial NAS message (i.e. REGISTRATION REQUEST message or SERVICE REQUEST message or CONTROL PLANE SERVICE REQUEST message, respectively), in the NAS message container IE of the SECURITY MODE COMPLETE message. The retransmitted CONTROL PLANE SERVICE REQUEST message:

a) shall not include any non-cleartext IE, except the Uplink data status IE; and

b) may include the Uplink data status IE.

If, prior to receiving the SECURITY MODE COMMAND message, the UE without a valid 5G NAS security context had sent a REGISTRATION REQUEST message the UE shall include the entire REGISTRATION REQUEST message in the NAS message container IE of the SECURITY MODE COMPLETE message as described in subclause 4.4.6.

If the UE operating in the single-registration mode receives the Selected EPS NAS security algorithms IE, the UE shall use the IE according to 3GPP TS 33.501 [24].

For a UE operating in single-registration mode in a network supporting N26 interface after an inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the UE shall set the value of the Selected EPS NAS security algorithms IE in the 5G NAS security context to the NAS security algorithms that were received from the source MME when the UE was in S1 mode.

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