**3GPP TSG-CT WG1 Meeting #136-eC1-22xxxx**

**lE-Meeting, 12th – 20th May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4304** | **rev** | **1** | **Current version:** | **17.6.1** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Abnormal cases for the SMC initiated for context synchronization between 3GPP access and non-3GPP access | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2022-05-16 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | According to Section 5.4.2.3, if a new 5G NAS security context is taken into use for one access in a network for a UE registered with a network over both 3GPP access and non-3GPP 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* toward the connected mode UE registered to the network via the other access as well.  However, it is not clear how the UE and the AMF operate if the UE had been in the connected mode until the SMC was initiated or was about to be initiated but has been in a condition in which the SMC cannot be completed or even initiated. For example,   1. For a UE registered with a network over both 3GPP access and non-3GPP access, the SECURITY MODE COMMAND message which includes the horizontal derivation parameter indicating "KAMF derivation is required" is sent over 3GPP access. 2. The UE is in the connected mode over non-3GPP access as well. 3. The AMF is about to send the SECURITY MODE COMMAND message over non-3GPP acces to activate the new 5G NAS security context that was activated over 3GPP access according to Secion 5.4.2.3, but the N1 signaling connection is lost over non-3GPP access; or The AMF actually sent the message but lower layer failure occurs; or The UE received the message over non-3GPP access and responded to the message but lower layer failure occurs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The UE and the AMF operate as if the UE has been in the idle mode over the non-current access. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It remains unclear how the UE and the AMF operate if the UE had been in the connected mode until the SMC is initiated but has gone idle before the SMC is completed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.3, 5.4.2.6, 5.4.2.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

#### 5.4.2.3 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.

If:

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

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

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

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

c) 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.

NOTE 1: If the UE was in 5GMM-CONNECTED mode over the non-current access when the new 5G NAS security context was taken into use for the current access and the UE enters 5GMM-IDLE mode over the non-current access before receiving a SECURITY MODE COMMAND message over the non-current access, the UE conforms to bullet a).

NOTE 2: If the UE was in 5GMM-CONNECTED mode over the non-current access when the new 5G NAS security context was taken into use and the N1 NAS signalling connection is lost over the non-current access before sending a SECURITY MODE COMMAND message over the non-current access, the AMF conforms to bullet a).

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.

NOTE 3: If the UE was in 5GMM-CONNECTED mode over the non-current access when the new 5G NAS security context was taken into use for the current access and the UE enters 5GMM-IDLE mode over the non-current access before receiving a SECURITY MODE COMMAND message over the non-current access, the UE conforms to bullet a).

NOTE 4: If the UE was in 5GMM-CONNECTED mode over the non-current access when the new 5G NAS security context was taken into use and the N1 NAS signalling connection is lost over the non-current access before sending a SECURITY MODE COMMAND message over the non-current access, the AMF conforms to bullet a).

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. satellite NG-RAN, 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.

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

#### 5.4.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication from lower layers (if the security mode control procedure is triggered by a registration procedure).

The UE shall abort the security mode control procedure and re-initiate the registration procedure.

b) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication with TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure).

If the current TAI is not in the TAI list, the security mode control procedure shall be aborted and a registration procedure shall be initiated.

If the current TAI is still part of the TAI list, the security mode control procedure shall be aborted and it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

c) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication without TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure).

The security mode control procedure shall be aborted and it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

d) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication from lower layers (if the previous security mode control procedure was completed over the non-current access and the UE is registered to a network over 3GPP access and non-3GPP access).

The UE shall abort the security mode control procedure and:

1) activate the new 5G NAS security context over the current access as described in 3GPP TS 33.501 [24]; and

2) set the downlink NAS COUNT and uplink NAS COUNT to zero for the current access, if:

i) the SECURITY MODE COMMAND message received over the non-current access includes the horizontal derivation parameter indicating "KAMF derivation is required"; or

ii) the SECURITY MODE COMMAND message received over the non-current access:

A) includes the horizontal derivation parameter indicating "KAMF derivation is not required"; or

B) does not include the Additional 5G security information IE; and

a primary authentication and key agreement procedure over the non-current access had been completed before receiving the SECURITY MODE COMMAND message over the non-current access.

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

#### 5.4.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure before the SECURITY MODE COMPLETE or SECURITY MODE REJECT message is received.

The network shall abort the security mode control procedure.

If the security mode control procedure was initiated via the current access in order to activate a new 5G NAS security context that had been activated over the non-current access for a UE which is registered to a network over 3GPP access and non-3GPP access (see subclause 5.4.2.3), the AMF shall:

1) activate the new 5G NAS security context over the current access as described in 3GPP TS 33.501 [24]; and

2) set the downlink NAS COUNT and uplink NAS COUNT to zero for the current access, if:

i) the SECURITY MODE COMMAND message sent over the non-current access includes the horizontal derivation parameter indicating "KAMF derivation is required"; or

ii) the SECURITY MODE COMMAND message sent over the non-current access:

A) includes the horizontal derivation parameter indicating "KAMF derivation is not required"; or

B) does not include the Additional 5G security information IE; and

a primary authentication and key agreement procedure over the non-current access had been completed before sending the SECURITY MODE COMMAND message over the non-current access.

b) Expiry of timer T3560.

The network shall, on the first expiry of the timer T3560, retransmit the SECURITY MODE COMMAND message and shall reset and start timer T3560. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3560, the procedure shall be aborted.

c) Collision between security mode control procedure and registration, service request or de-registration procedure not indicating switch off.

The network shall abort the security mode control procedure and proceed with the UE initiated procedure.

d) Collision between security mode control procedure and other 5GMM procedures than in item c.

The network shall progress both procedures.

e) Lower layers indication of non-delivered NAS PDU due to handover:

If the SECURITY MODE COMMAND message could not be delivered due to an intra AMF handover and the target TA is included in the TAI list, then upon successful completion of the intra AMF handover the AMF shall retransmit the SECURITY MODE COMMAND message. If a failure of the handover procedure is reported by the lower layer and the N1 signalling connection exists, the AMF shall retransmit the SECURITY MODE COMMAND message.

\* \* \* End of Changes \* \* \* \*