**3GPP TSG-CT WG1 Meeting #123-eC1-202626**

**Electronic meeting, 16-24 April February 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **2150** | **rev** | **1** | **Current version:** | **16.4.1** |  |
|  | | | | | | | | |
| *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:*** | Retransmission of a CPSR message after integrity check failure at the AMF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_CIoT | | | | |  | ***Date:*** | | | 2020-04-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The WB-N1 mode UE which uses CP IoT 5GS optimization and has an emergency PDU sesssion may send data in the clear when retransmitting the unciphered CPSR message (with data) in the Security Mode Complete message resulting from a failed integrity check on the initial CPSR message that was sent. See C1-202403.  To avoid sending CIoT data in the clear, the UE should ensure that the CPSR message which gets included in the NAS message container IE of the Security Mode Complete message does not include data. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update section 5.4.2.3 to also consider the CPSR message. Furthermore:   * the CPSR message that the UE includes in the NAS message container IE of the Security Mode Complete message should not contain any non-cleartext IE   Update section 5.4.2.4 to consider the CPSR message | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UE will send SMS, CP data or location services message with no protection which exposes user data that is related to an unauthenticted emergency session. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.3, 5.4.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\* START CHANGE \*\*\*\*\*\*\*\*

#### 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 and 5.4.1.2.3A.1.

If:

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

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

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.

Editor's note (WI:5WWC, CR# 2020): The EAP details e.g. on ngKSI and ABBA for N5GC devices are FFS based on what will be specified by SA WG3.

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 SERVICER REQUEST message, respectively), in the NAS message container IE of the SECURITY MODE COMPLETE message. The CONTROL PLANE SERVICE REQUEST message shall not include any non-cleartext 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.

\*\*\*\*\*\*\*\* START CHANGE \*\*\*\*\*\*\*\*

#### 5.4.2.4 NAS security mode control completion by the network

The AMF shall, upon receipt of the SECURITY MODE COMPLETE message, stop timer T3560. From this time onward the AMF shall integrity protect and encipher all signalling messages with the selected 5GS integrity and ciphering algorithms.

If the SECURITY MODE COMPLETE message contains a NAS message container IE with a REGISTRATION REQUEST message, the AMF shall complete the ongoing registration procedure by considering the REGISTRATION REQUEST message contained in the NAS message container IE as the message that triggered the procedure.

If the SECURITY MODE COMPLETE message contains a NAS message container IE with a REGISTRATION REQUEST message, the 5GMM capability IE included in the REGISTRATION REQUEST message indicates "S1 mode supported" and the AMF supports N26 interface, the AMF shall initiate another NAS security mode control procedure in order to provide the selected EPS NAS security algorithms to the UE as described in subclause 5.4.2.2.

If the SECURITY MODE COMPLETE message contains a NAS message container IE with a SERVICE REQUEST message, the AMF shall complete the ongoing service request procedure by considering the SERVICE REQUEST message contained in the NAS message container IE as the message that triggered the procedure.

If the SECURITY MODE COMPLETE message contains a NAS message container IE with a CONTROL PLANE SERVICE REQUEST message, the AMF shall complete the ongoing service request procedure by considering the CONTROL PLANE SERVICE REQUEST message contained in the NAS message container IE as the message that triggered the procedure.