**3GPP TSG-CT WG1 Meeting #126-eC1-206007-revTBD**

**Electronic meeting, 15-23 October 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **2662** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Uplink data status IE in CPSR after integrity check failure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17, 5G\_CIoT | | | | |  | ***Date:*** | | | 2020-10-02 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | After the integrity check on CPSR fails and the UE has a PDU session for emergency services, the UE currently sends a CPSR message with no cleartext IE.  However, the purpose of the CPSR message can be to request user-plane resources for the emergency PDU session. Therefore, the Uplink data status IE should be included in the CPSR message because:  1) the UE needs to request user-plane resources for the the emergency PDU session,  2) the Uplink data status IE which does not reveal any privacy information.  Note: the same can happen with the Service Request message for which the UE **is actually allowed to send the Uplink data status IE** as described below from section 5.4.2.2:  “If, during an ongoing service request procedure for a UE with an emergency PDU session, the AMF is initiating a SECURITY MODE COMMAND (i.e. after receiving the SERVICE REQUEST message, but before sending a response to that message) and the SERVICE REQUEST message does not successfully pass the integrity check at the AMF, the AMF shall include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message **requesting the UE to send the entire SERVICE REQUEST message in the SECURITY MODE COMPLETE message** as described in 3GPP TS 33.501 [24].”  Also, looking at the text fom section 5.4.2.2 that is shown above, the text needs to be updated to also include the CPSR message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The UE can send the Uplink data status IE in the CPSR message that is sent following a failed integrity check only when the UE has an emergeny PDU session. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UE cannot request user-plane resources for the emergeny PDU session after the integrity check fails in the network. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.2, 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:*** | | (a) The WI is changed to “5GProtoc17, 5G\_CIoT”  (b) The CR category is changed from “A” to “F”, hence only purused in Rel-17 | | | | | | | | |

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

#### 5.4.2.2 NAS security mode control initiation by the network

The AMF initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer T3560 (see example in figure 5.4.2.2).

The AMF shall reset the downlink NAS COUNT counter and use it to integrity protect the initial SECURITY MODE COMMAND message if the security mode control procedure is initiated:

a) to take into use the security context 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) upon receipt of REGISTRATION REQUEST message, if the AMF needs to create a mapped 5G NAS security context (i.e. the type of security context flag is set to "mapped security context" in the NAS key set identifier IE included in the SECURITY MODE COMMAND message).

The AMF shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the 5G NAS integrity key based on KAMF or mapped K'AMF indicated by the ngKSI included in the message. The AMF shall set the security header type of the message to "integrity protected with new 5G NAS security context".

The AMF shall create a locally generated KAMF and send the SECURITY MODE COMMAND message including an ngKSI value in the NAS key set identifier IE set to "000" and 5G-IA0 and 5G-EA0 as the selected NAS security algorithms only when the security mode control procedure is initiated:

a) during an initial registration procedure for emergency services if no shared 5G NAS security context is available;

b) during a registration procedure for mobility and periodic registration update for a UE that has an emergency PDU session if no shared 5G NAS security context is available;

c) during a service request procedure for a UE that has an emergency PDU session if no shared 5G NAS security context is available; or

d) after a failed primary authentication and key agreement procedure procedure for a UE that has an emergency PDU session or is establishing an emergency PDU session, if continued usage of a shared 5G NAS security context is not possible.

When the AMF sends the SECURITY MODE COMMAND message including an ngKSI value in the NAS key set identifier IE set to "000" and 5G-IA0 and 5G-EA0 as the selected NAS security algorithms, if:

a) the AMF supports N26 interface;

b) the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message; and

c) the security mode control procedure is initiated during an initial registration procedure for emergency services, during a registration procedure for mobility and periodic registration update for a UE that has an emergency PDU session, or during a service request procedure for a UE that has an emergency PDU session,

the SECURITY MODE COMMAND message shall also include the Selected EPS NAS security algorithms IE. The selected EPS NAS security algorithms shall be set to EIA0 and EEA0.

The UE shall process a SECURITY MODE COMMAND message including an ngKSI value in the NAS key set identifier IE set to "000" and 5G-IA0 and 5G-EA0 as the selected NAS security algorithms and, if accepted, create a locally generated KAMF when the security mode control procedure is initiated:

a) during an initial registration procedure for emergency services;

b) during a registration procedure for mobility and periodic registration update for a UE that has an emergency PDU session;

c) during a service request procedure for a UE that has an emergency PDU session; or

d) after a primary authentication and key agreement procedure procedure for a UE that has an emergency PDU session or is establishing an emergency PDU session.

NOTE 1: The process for creation of the locally generated KAMF by the AMF and the UE is implementation dependent. The KAMF is specified in 3GPP TS 33.501 [24].

Upon receipt of a REGISTRATION REQUEST message, if the AMF does not have the valid current 5G NAS security context indicated by the UE, the AMF shall either:

a) indicate the use of the new mapped 5G NAS security context to the UE by setting the type of security context flag in the NAS key set identifier IE to "mapped security context" and the KSI value related to the security context of the source system; or

b) set the ngKSI value "000" in the NAS key set identifier IE if the AMF sets 5G-IA0 and 5G-EA0 as the selected NAS security algorithms for a UE that has an emergency PDU session.

While having a current mapped 5G NAS security context with the UE, if the AMF needs to take the native 5G NAS security context into use, the AMF shall include the ngKSI that indicates the native 5G NAS security context in the SECURITY MODE COMMAND message.

The AMF shall include the replayed security capabilities of the UE (including the security capabilities with regard to NAS, RRC and UP (user plane) ciphering as well as NAS and RRC integrity, and other possible target network security capabilities, i.e. E-UTRAN if the UE included them in the message to network), the selected 5GS ciphering and integrity algorithms and the ngKSI.

If a UE is already registered over one access to a PLMN and the AMF decides to skip primary authentication and key agreement procedure when the UE attempts to register over the other access to the same PLMN, the AMF shall take into use the UE's current 5G NAS security context over the other access that the UE is registering. In this case, SECURITY MODE COMMAND message is not sent to the UE.

If the UE is registered to the same AMF and the same PLMN over both 3GPP access and non-3GPP access, and the UE is in 5GMM-CONNECTED mode over both the 3GPP and non-3GPP accesses, then at any time the primary authentication and key agreement procedure has successfully completed over:

a) the 3GPP access, the AMF includes the ngKSI in the SECURITY MODE COMMAND message over the 3GPP access. When the AMF sends the SECURITY MODE COMMAND message to UE over the non-3GPP access to take into use the new 5G NAS security context, the AMF shall include the same ngKSI in the SECURITY MODE COMMAND message to identify the new 5G NAS security context; or

b) the non-3GPP access, the AMF includes the ngKSI in the SECURITY MODE COMMAND message over the non-3GPP access. When the AMF sends the SECURITY MODE COMMAND message to UE over the 3GPP access to take into use the new 5G NAS security context, the AMF shall include the same ngKSI in the SECURITY MODE COMMAND message to identify the new 5G NAS security context.

The AMF may initiate a SECURITY MODE COMMAND in order to change the 5G security algorithms for a current 5G NAS security context already in use. The AMF re-derives the 5G NAS keys from KAMF with the new 5G algorithm identities as input and provides the new 5GS algorithm identities within the SECURITY MODE COMMAND message. The AMF shall set the security header type of the message to "integrity protected with new 5G NAS security context".

If, during an ongoing registration procedure, the AMF is initiating a SECURITY MODE COMMAND (i.e. after receiving the REGISTRATION REQUEST message, but before sending a response to that message) and:

a) the REGISTRATION REQUEST message does not successfully pass the integrity check at the AMF; or

b) the AMF can not decipher the value part of the NAS message container IE in the REGISTRATION REQUEST message;

the AMF shall include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message requesting the UE to send the entire REGISTRATION REQUEST message in the SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24].

If, during an ongoing service request procedure for a UE with an emergency PDU session, the AMF is initiating a SECURITY MODE COMMAND (i.e. after receiving the SERVICE REQUEST message or the CONTROL PLANE SERVICE REQUEST message, but before sending a response to that message) and the SERVICE REQUEST message or the CONTROL PLANE SERVICE REQUEST message does not successfully pass the integrity check at the AMF, the AMF shall include the Additional 5G security information IE with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message requesting the UE to send the entire:

a) SERVICE REQUEST message; or

b) CONTROL PLANE SERVICE REQUEST message excluding non-cleartext IEs, except the Uplink data status IE if needed (see subclause 5.4.2.3);

in the SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24].

Additionally, the AMF may request the UE to include its IMEISV in the SECURITY MODE COMPLETE message.

If the AMF supports N26 interface and the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message, the AMF shall select ciphering and integrity algorithms to be used in the EPS and indicate them to the UE via the Selected EPS NAS security algorithms IE in the SECURITY MODE COMMAND message.

NOTE 2: The AS and NAS security capabilities are the same, i.e. if the UE supports one algorithm for NAS, the same algorithm is also supported for AS.

If the AMF performs horizontal key derivation e.g. during the mobility and periodic registration update or when the UE is already registered in the PLMN with another access type as described in 3GPP TS 33.501 [24], the AMF shall include horizontal derivation parameter in the SECURITY MODE COMMAND message.

If the security mode control procedure is initiated after successful EAP based primary authentication and key agreement procedure and the security mode control procedure intends to bring into use the partial native 5G NAS security context created by the EAP based primary authentication and key agreement procedure, the AMF shall set the EAP message IE of the SECURITY MODE COMMAND message to an EAP-success message to be sent to the UE.



Figure 5.4.2.2: Security mode control procedure

\*\*\*\*\* 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.

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;

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 CHANGE \*\*\*\*\*\*