**3GPP TSG-CT WG1 Meeting #127-eC1-207509**

**Electronic meeting, 13-20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **2870** | **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 |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification on Selected EPS NAS security algorithms IE | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc17 | | | | |  | ***Date:*** | | | 2020-11-04 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The following is stated regarding the Selected EPS NAS security algorithms IE in 5.4.2.2:  “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.”  The above means that everytime the AMF sends the SECURITY MODE COMMAND message, then the AMF shall also send the Selected EPS NAS security algorithms IE. However, this is not the case since the AMF may decide to change the 5G NAS security algorithms but may not necessarily change the selected EPS NAS security algorithms.  Therefore the text needs to be modified accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that if the AMF is initiating the procedure to provide the Selected EPS NAS security algorithms IE, then the IE shall be included in the message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The AMF that supports N26 interface will always send the IE for a UE that supports S1 mode which is unnecessary if the SMC is sent to only modify the 5G NAS security algorithms. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.2, 8.2.25.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*

#### 5.4.2.2 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, 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].

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

If the AMF is initiating the procedure to provide the selected EPS NAS security algorithms to the UE, 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 \*\*\*\*\*

#### 8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included if the AMF supports N26 interface, the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message, and the AMF needs to provide the selected EPS NAS security algorithms to the UE.

\*\*\*\*\* END CHANGE \*\*\*\*\*