

Discussion on Selected EPS NAS algorithm delivery

MediaTek Inc.

Problem statement 1/3

Condition to provide the UE with the 'Selected EPS NAS algorithms' IE are

- The AMF supports N26 interface; and
- The UE has set 'S1 mode supported' bit as true in 5GMM capability IE in REGISTRATION REQUEST

9.11.3.1 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 9.11.3.1.1 and table 9.11.3.1.1.

The 5GMM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

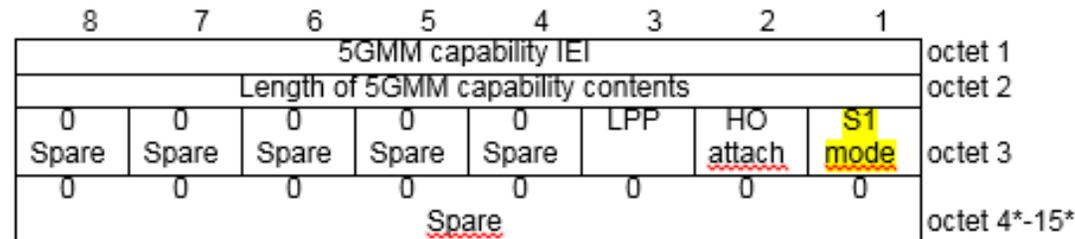


Figure 9.11.3.1.1: 5GMM capability information element

Problem statement 2/3

Problem at initial registration

- 5GMM capability IE is a "non-plaintext IE"
- Entire REGISTRATION REQUEST message containing also "non-plaintext IEs" is sent to the AMF at SECURITY MODE COMPLETE message
- The AMF cannot provide the Selected EPS NAS algorithms to the UE at SECURITY MODE COMMAND message
- Second round of SMC is needed to provide the "Selected EPS NAS algorithms" to the UE

Table 8.2.25.1.1: SECURITY MODE COMMAND message content

8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included 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.

Problem statement 3/3

Current approach in TS 24.501 Rel-16

“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.”

For signalling efficiency a solution should be provided for Rel-16.

Proposed alternative solutions 1/2

Solution Alt#1

- Report “S1 mode supported” always as a cleartext in REGISTRATION message
 - Sending complete “5GMM capability IE” as a cleartext; or
 - Sending new “S1 mode supported IE” or “EPS capability IE” as a cleartext

Solution Alt#2

- Always send “Selected EPS NAS algorithms” IE if the AMF has support for N26 interface regardless of an UE “S1 mode supported” status
 - The UE has always Selected EPS NAS algorithms
 - The UE not supporting S1 mode can ignore the Selected EPS NAS algorithms IE

Proposed alternative solutions 2/2

Solution Alt#3

- Report “Selected EPS NAS security algorithms” IE in REGISTRATION ACCEPT message after the AMF has received complete REG REQ with “S1 mode supported” indication

Proposal

- CT1 to discuss and decide whether the problem needs to be fixed in Rel-16
- If CT1 agrees the problem needs to be fixed, CT1 selects one of the proposed alternatives #1, #2 or #3 as way forward
- MediaTek prefers either solution Alt#2 or Alt#3 as way forward
- MediaTek Inc. volunteers to write a CR for 24.501 to solve the problem
 - Solution Alt#1: see C1-203584
 - Solution Alt#2: see C1-203585
 - Solution Alt#3: see C1-203586

References 1/2

- 3GPP TS 33.501 - '6.7.2 NAS security mode command procedure':
 - 1b The AMF sends the NAS Security Mode Command message to the UE. The NAS Security Mode Command message shall contain: the replayed UE security capabilities, **the selected NAS algorithms**, and the ngKSI for identifying the KAMF.
 - In case the network supports interworking using the N26 interface between MME and AMF, the AMF shall also include the selected EPS NAS algorithms (defined in Annex B of TS 33.401 [10]) to be used after mobility to EPS in the NAS Security Mode Command message (see clause 8.5.2). The UE shall store the algorithms for use after mobility to EPS using the N26 interface between MME and AMF. The AMF shall store the selected EPS NAS algorithms in the UE security context.
- 3GPP TS 24.501 – '6.7.2 NAS security mode command procedure'
 - 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.

References 2/2

- SELECTED EPS NAS security algorithms will be indicated when “S1 mode supported”

8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included 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.

- S1_MODE was a part of 5GMM capability and **not** in cleartext IEs align to 3gpp ts24.501
 - *24.501 sec 9.11.3.1*

9.11.3.1 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 9.11.3.1.1 and table 9.11.3.1.1.

The 5GMM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

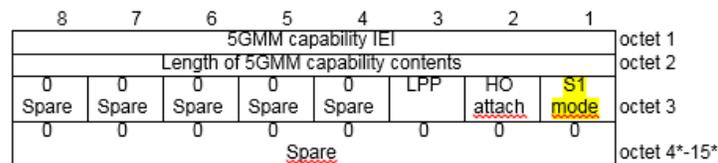


Figure 9.11.3.1.1: 5GMM capability information element