**3GPP TSG-SA3 Meeting #100e-Bis *S3-202667***

**e-meeting, 12 -16 october 2020**

**Title:** LS on Clarification on processing of messages after NAS security establishment

**Response to:**

**Release:** Rel-17

**Work Item:** FS\_AMFREAL\_SEC

**Source:** SA3

**To:** CT1

**Cc:** SA2

**Contact Person:**

#### Name: Suresh Nair

**Tel. Number:**

E-mail Address: suresh.p.nair@nokia.com

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:**

**1. Overall Description:**

SA3 is conducting a study on the security issues of AMF re-allocation ([SP-200721](https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=SP-200721','SP-200721)), where an initial AMF may need to reroute the UE’s registration request to a target AMF.

SA3 has a clarification question on the list of messages the UE would accept without integrity protection.

TS 24.501 clause 4.4.4.2 contains the following description:

#### 4.4.4.2 Integrity checking of NAS signalling messages in the UE

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

a) IDENTITY REQUEST (if requested identification parameter is SUCI);

b) AUTHENTICATION REQUEST;

c) AUTHENTICATION RESULT;

d) AUTHENTICATION REJECT;

e) REGISTRATION REJECT (if the 5GMM cause is not #76);

f) DEREGISTRATION ACCEPT (for non switch off); and

g) SERVICE REJECT (if the 5GMM cause is not #76).

NOTE: These messages are accepted by the UE without integrity protection, as in certain situations they are sent by the network before security can be activated.

….

Once the secure exchange of NAS messages has been established, the receiving 5GMM entity in the UE shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS in the UE shall discard that message. The processing of the SECURITY MODE COMMAND message that has not successfully passed the integrity check is specified in subclause 5.4.2.5. If any NAS signalling message is received as not integrity protected even though the secure exchange of NAS messages has been established by the network, then the NAS shall discard this message.

The description in the first sentence “, *unless the network has established secure exchange ..”,*  the NOTE and the context below the NOTE leads to different interpretations.

Particularly SA3 would like to understand whether the messages listed above a) to g) can still be processed by UE, after the secure exchange of NAS messages has been established e.g. using a NAS SMC procedure.

**2. Actions:**

**To CT1 group.**

**ACTION:** SA3 kindly asks CT1 group to answer the above question.

**3. Date of Next TSG-SA WG3 Meetings:**

SA3#101e 9 - 20 November 2020 e-meeting

SA3#101bis-e 18 – 22 January 2021 e-meeting