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

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

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

**Response to:**

**Release:**

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

**Source:** To be 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**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

**1. Overall Description:**

SA3 is conducting a study on the issue 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 transfer the UE context to a target AMF, support correct Network Slice, to provide optimal services to the UE etc.

In this regard, SA3 have a clarification question on the list of messages the UE would accept without integrity protection, after NAS security context have been established between the UE and an initial AMF.

TS 24.501 clause 4.4.4.2 contains a list of messages with an unclear exception clause, which is quoted below.

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 neither #31 nor #76);

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

g) SERVICE REJECT (if the 5GMM cause is neither #31 nor #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.

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

Particularly SA3 would like to understand whether an authenticated UE, after security establishment using a NAS SMC procedure between an AMF, would accept and respond to an unprotected IDENTITY REQUEST (if requested identification parameter is SUCI) from another AMF.

**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 TBD 2020 e-meeting