**3GPP TSG-SA3 Meeting #103-e *S3-212124***

e-meeting, 17 - 28 May 2021

**Title: LS on Clarifications of Network slice selection during AMF Reallocation**

**Response to: N/A**

**Release: Rel. 17**

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

**Source: Lenovo, Motorola Mobility to be SA3**

**To: SA2, CT1**

**Cc: -**

**Contact person: Sheeba Backia Mary Baskaran**

 **smary@lenovo.com**

 **017411977172**

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

**Attachments:** TR 33.864

# 1 Overall description

SA3 is currently working on the "Study on the security of Access and Mobility Management Function (AMF) re-allocation" in TR 33.864. The study is focusing on addressing the security handling related to AMF re-allocation and indirect reroute via RAN specified in TS 23.502 Clause 4.2.2.2.3 "Registration with AMF re-allocation", option 7(B). According to the procedure, if the initial AMF (which received the UE registration Request) finds that it is not capable to serve a UE then the registration request will be rerouted to the selected target AMF via RAN and the initial AMF will provide the information (such as AMF set and Allowed NSSAI) to enable the RAN to select the suitable target AMF.

The problem with the existing AMF reallocation and reroute via RAN procedure is the following. During the registration procedure with SUCI or 5G-GUTI, if the initial AMF sets up NAS security with UE soon after the primary authentication and if determines that "an AMF reallocation and Reroute via RAN" is required, then after the rerouting of registration request to the target re-allocated AMF, all unprotected NAS message sent by the re-allocated target AMF to the UE (ex. to initiate an Authentication) will not be processed by the UE. In this case, the registration would fail subsequently as the UE which has established a secure NAS exchange with the initial AMF will not process any unprotected NAS message sent by the re-allocated target AMF.

## 1.1 SA2 Background information

In the procedure of Registration with AMF re-allocation (TS 23.502, 4.2.2.2.3), the initial AMF queries NSSF (i.e., using Nnssf\_NSSelection\_Get service operation given in TS 23.502) with inputs such as Requested NSSAI, Subscribed NSSAI etc. According to TS 23.502 Clause 5.2.16.2.1 "Nnssf\_NSSelection\_Get service operation", if the service operation is invoked during Registration procedure for Network Slice selection, the Requested NSSAI is provided as an optional IE and the subscribed NSSAI as the mandatory IE among other inputs.

## 1.2 CT1 Background information

The CT1 TS 24.501, clause 5.4.1.2 "EAP based primary authentication and key agreement procedure, states the following:

*If the authentication of the UE completes successfully and the serving AMF does not intend to initiate a security mode control procedure bringing into use the partial native 5G NAS security context created by the EAP based primary authentication and key agreement procedure, then the EAP-success message, and the ngKSI are transported from the network to the UE using the AUTHENTICATION RESULT message of the EAP result message transport procedure.*

*NOTE 1: The serving AMF will not initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure e.g. in case of AMF relocation during registration procedure.’*

## 1.3 Questions

To solve the above repeated registration failure issue, SA3 is considering solutions 6 and 7 from the TR 33.864 that have the following points as their core principle, which need to be evaluated by SA2 and CT1:

1. The initial AMF uses the Requested NSSAI (if available to the AMF) and subscribed NSSAI along with existing information/inputs for Network slice selection using Nnssf\_NSSelection\_Get service operation defined in TS 23.502.

2. The initial AMF uses no Requested NSSAI (if not available to the AMF) and uses subscribed NSSAI along with existing information for Network slice selection using Nnssf\_NSSelection\_Get service operation defined in TS 23.502. In this case, the initial AMF does not attempt to perform NAS SMC to fetch Requested NSSAI provided by UE for the sake of performing network slice selection.

3. If the initial AMF determines that "an AMF reallocation and reroute via RAN" is required based on TS 23.502, clause 4.2.2.2.3, then the initial AMF does not perform NAS SMC with the UE (i.e., even if the Requested NSSAI is not available at the initial AMF, where the UE may have provided the Requested NSSAI in the protected mobility update registration Request to the initial AMF and the initial AMF couldn’t decipher/ identify the UE with the 5G-GUTI. Instead the initial AMF uses the existing Nnssf\_NSSelection\_Get service operation with Requested NSSAI as optional IE and uses all other essential and mandatory inputs (ex., subscribed NSSAIs etc)).

Therefore, a clarification from the respective group would be much helpful for the SA3 WG to evaluate the working feasibility of solution 6 and 7 accordingly.

Based on the above information we would like to know the views from SA2 and CT1 respectively.

* **Question 1 to SA2:** Is it feasible for the initial AMF during a registration procedure with SUCI to perform network slice selection using Nnssf\_NSSelection\_Get service operation without Requested NSSAI, but using all other existing IE as inputs (e.g., subscribed NSSAI etc.) ?
* **Question 2 to SA2:** Is it feasible for the initial AMF during registration with 5G-GUTI to perform network slice selection using Nnssf\_NSSelection\_Get service operation without Requested NSSAI, but using other existing IE as inputs (e.g., subscribed NSSAI etc.)?
* **Question 3 to SA2:** Can the solutions 6 and 7 meet the SA2 working principles for the AMF re-allocation and reroute via RAN and related network slice selection principles?
* **Question 1 to CT1:** Can SA3 consider the following NOTE 1 from TS 24.501 Clause 5.4.1.2 as a valid principle for the ongoing SA3 "Study on the security of Access and Mobility Management Function (AMF) re-allocation"?

*NOTE 1: The serving AMF will not initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure e.g. in case of AMF relocation during registration procedure.*

* **Question 2 to CT1:** Does the aforementioned NOTE 1 refer to the NAS SMC following a primary authentication between UE and initial AMF (or) does it refer to the NAS SMC following a primary authentication between UE and the reallocated target AMF (following the reroute).

# 2 Actions

**To SA2:**

**ACTION:** 3GPP TSG SA WG3 kindly asks SA2 to answer the above SA2 related questions .

**To CT1:**

**ACTION:** 3GPP TSG SA WG3 kindly asks CT1 to answer the above CT1 related questions.

# 3 Dates of next TSG SA WG 3 meetings

SA3#103Bis-e 5 - 9 ~July 2021 Electronic meeting (TBC)

SA3#104-e 16 - 27 August 2021 Electronic meeting