**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230193***

**Electronic meeting, 16 - 20 January 2023**

**Source: Huawei, HiSilicon**

**Title: Adding solution on KI#4**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] 3GPP TR 33.887: "Study on Security aspects for 5WWC Phase 2".

# 3 Rationale

*To solve the mobility problem of TNAP, the solution enables UE to generate different keys when moving between different TNAPs*

This solution proposes to define a new ERP-like procedure called EAP 5G Restart, i.e. the UE and the TNGF generates a reauthentication root key and perfroms the reauthentication between the UE and TNGF.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

## 6.X Solution #X: TNAP mobility solution without full authentication

### 6.X.1 Introduction

This solution addresses key issue #4: Security aspect of TNAP mobility

### 6.X.2 Solution details

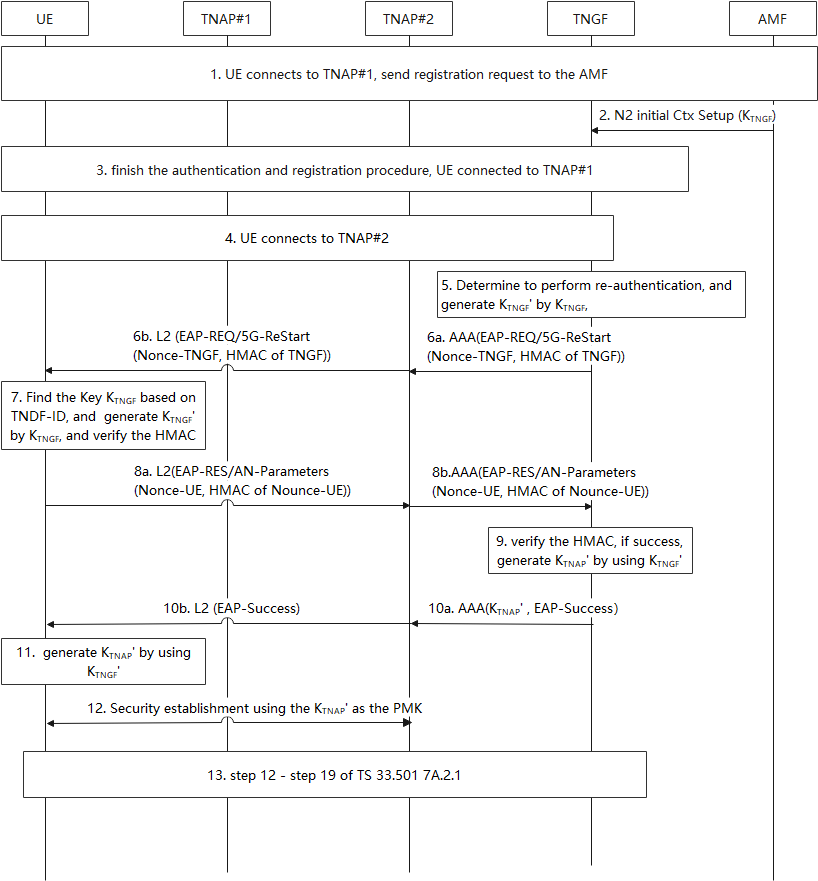


Figure 6.X.2-1: TNAP mobility procedure

1-3. UE connected to TNAP#1 by performing the procedure defined in TS33.501 7A.2.1 step1- step19.

4. The TNGF knows the UE reconnect to the TNGF again, but via TNAP#2 by receving the same UE ID in the previous connection. The UE ID is the SUCI or 5G-GUTI used in step1.

5. TNGF finds the UE security context based on the UE ID, and determines to perform re-authentication procedure based on UE ID. The TNGF generates KTNGF’ that is equlivant to the EAP 5G reauthentication root key by using the method in A.22 of TS 33.501[xx] with the usage type distinguisher set to 0x03, with the input key KTNGF

Editor’s Note: whether the additional key is needed if FFS.

6. TNGF sends EAP-REQ message to start the re-authentication procedure, a,Nonce-TNGF and the HMAC are carried in this message. HMAC is generated by using fresh parameter and KTNGF’. TNAP#2 forwawrd this message to UE.

7. UE finds the KTNGF by using TNGF ID in step 4, and generates KTNGF’ by using the same method in step5, and verifies the HMAC. if the verification passes, perform next steps.

8. UE sends EAP-RES message, Nonce-UE and HMAC are carried in AN-Parameters of this message, HMAC is generated by using Nonce-UE parameter and KTNGF’ , TNAP#2 forward this message to TNGF.

9. TNGF verifies the HMAC, if the verification passes, TNGF generates KTNAP’ by using method defined in TS33.501 A.22.

10. TNGF sends EAP-Success message to TNAP#2, KTNAP’ generated in step 9 is carried in this message. TNAP#2 forwawrd EAP-Success message to UE.

11. After receiving EAP-Success message, UE generates KTNAP’ by using the same method in step 9.

12. UE and TNAP#2 establish security association by using the newly generated KTNAP’.

13. TS33.501 7A.2.1 step12- step19.

### 6.X.3 Evaluation

This solution addresses the requirement of KI #4 by generating a new KTNGF’.

This solution impacts UE and TNGF without affecting other NFs.

Editor’s Note: Further evaluation is FFS.

\*\*\* END OF 1st CHANGE\*\*\*