**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222691-r2***

**e-meeting, 10 - 14 October 2022**

**Source: CableLabs**

**Title: EAP base authentication for AUN3 devices behind RG in SNPN**

**Document for: Approval**

**Agenda Item: 5.13**

# 1 Decision/action requested

***It is requested to approve the pCR.***

# 2 References

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

[Y]            3GPP TS 33.501: "Security architecture and procedures for 5G System"

[Z] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

# 3 Rationale

This pCR proposes a solution for KI#1 in TR 33.887 [X] to authenticate AUN3 device connecting to RG in SNPN. This solution fills the following gaps in Annex O:

1. it allows 5G-RG to register AUN3 device to 5GC on its behalf, while in Annex O, it is always the W-AGF that registers N5GC device to the 5GC.

2. it allows the AUN3 device to authenticate and connect to RG via WiFi by using the MSK from the EAP authentication between the AUN3 device and the AUSF. In Annex O, the N5GC device only connects to the RG via wireline (e.g., Ethernet) and no crypto key is sent back by the AUSF to the RG to facilitate WiFi four-way handshaking.

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 6.Y Solution #Y: EAP base authentication for AUN3 devices behind RG in SNPN

### 6.Y.1 Introduction

This solution defines an authentication procedure for AUN3 devices behind RG (5G-RG or FN-RG) in SNPN. It differs from Annex O of TS 33.501 [Y] in that:

1. it allows 5G-RG to register AUN3 device to 5GC on its behalf, while in Annex O, it is always the W-AGF that registers N5GC device to the 5GC.

2. it allows the AUN3 device to connect to RG via WiFi based on the MSK from the EAP authentication between the AUN3 device and the AUSF. In Annex O, the N5GC device connects to the RG via wireline (e.g., Ethernet) and MSK is not sent back by the AUSF to the RG to facilitate WiFi four-way handshaking.

### 6.Y.2 Solution details



1. The AUN3 device attempts to establish a layer 2 connection with the RG either via Ethernet or WiFi. If the layer 2 connection is based on Ethernet, steps 13-14 are skipped.

2. The RG initiates the EAP authentication procedure by sending an EAP request/Identity to the AUN3 device in a layer frame (e.g., EAPOL).

3. The AUN3 device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

Editor’s Note: subscription identifier privacy protection is FFS.

4a-4b. If the RG is an FN-RG, the FN-RG sends the EAP response/Identity including the NAI to the W-AGF. The W-AGF constructs a SUCI from NAI-based SUPI using NULL scheme and sends a NAS Registration Request message to the AMF, including the SUCI and AUN3 device indicator.

4c. If the RG is a 5G-RG, the 5G-RG constructs a SUCI from the NAI-based SUPI of the AUN3 device, and sends a NAS Registration Request message to the AMF, including the SUCI and an AUN3 device indicator.

5. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the AUN3 device, and an AUN3 device indicator.

6. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the AUN3 device and the AUN3 device indicator.

7. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method based on the SUPI. When the "username" part of the SUPI is "anonymous" or omitted, the UDM may select an authentication method based on the “realm” part of the SUPI, the AUN3 device indicator, a combination of the "realm" part and the AUN3 device indicator, or the UDM local policy.

8. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains the SUPI of the AUN3 device and an indicator of the selected authentication method. EAP-AKA’ as specified in RFC 5448 [Z] or other key generating EAP method can be selected.

9. The AUSF and the AUN3 device perform EAP authentication based on the selected authentication method. Storage and processing of credentials for EAP authentication method is described in Annex I of TS 33.501 [Y].

10. If the EAP authentication between the AUSF and the AUN3 device is completed successfully, the AUSF sends to the AMF/SEAF an EAP-Success message along with the SUPI and the MSK in a Nausf\_UEAuthentication\_Authenticate Response message.

11a-11b. If steps 4a-4b is executed, the AMF/SEAF sends to the W-AGF the EAP-Success message and the MSK in an Authentication Result message. The W-AGF sends to the FN-RG the EAP-Success message and the MSK in AAA message.

11c. If step 4c is executed, the AMF/SEAF sends to the 5G-RG the EAP-Success message and the MSK in an Authentication Result message.

12. The RG sends to the AUN3 device the the EAP-Success message in a layer 2 frame.

13a-13b. The AUN3 device and the RG use the first 256-bit of the MSK as the PMK, from which the WLAN keys are derived.

14. The AUN3 and the RG performs four-way handshaking to establish WLAN secure connection.

### 6.Y.3 Evaluation

This solution meets the requirement that an AUN3 device connecting to RG shall be able to authenticate to 5GC.

**\*\*\*\*** END OF CHANGE **\*\*\*\***