**3GPP TSG-SA3 Meeting #116S3-241874**

**Jeju, South Korea, 20th - 24th May 2024**

**Source: CableLabs**

**Title: Solution for authentication and authorization of non-3GPP devices behind 5G-RG**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is requested to approve the new solution in this pCR.***

# 2 References

[X] 3GPP TS 33.501 " Security architecture and procedures for 5G system"

[Y] 3GPP TR 33.700-32 " Study on security aspects of User Identities and Authentication"

3 Rationale

This contribution proposes a solution for the KI #3 in TR 33.700-32 [Y] for authorization of non-3GPP devices behind gateway UE or 5G-RG.

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.700-32 [Y].

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

6.X Solution #X: authorization of non-3GPP devices behind 5G-RG

6.X.1 Introduction

This solution addresses Key Issue #3 on the authorization of non-3GPP devices behind 5G-RG. It is based on the authentication of FN-RG in clause 7B.3 of TS 33.501 [X], with additional authorization check that the non-3GPP device is under the control of an RG which has been successfully authenticated by 5GC. This ensures that an RG can only represent an non-3GPP device allowed by the RG subscription.

Editor’s note: Clarification of changes from clause 7B.3 is FFS.

6.X.2 Solution details



Figure 6.X.2-1. authorization of non-3GPP devices behind 5G-RG

1. A layer-2 (L2) connection is established between the non-3GPP device and the 5G-RG using local authentication (e.g., WPA personal).

2. The 5G-RG sends an AAA message to the W-AGF to indicate that a device with a non-3GPP device identifier has been successfully authenticated locally.

Note1. The identifier of the non-3GPP device is defined by BBF or CableLabs and is out of scope of 3GPP.

3. The W-AGF sends back a confirmation AAA message to the RG.

Note2. The AAA messages used between the 5G-RG and the W-AGF in steps 2-3 are defined by BBF or CableLabs and out of scope of 3GPP.

4. The W-AGF shall perform initial registration on behalf of the non-3GPP device. The W-AGF shall generate a Registration Request message and send it to the AMF over N2. The Registration Request message contains the SUCI of the non-3GPP device and the SUCI of the 5G-RG. The N2 message contains an indication that the RG has authenticated the non-3GPP device.

Editor’s Note: whether the non-3GPP device is required to register to the 5GC is ffs and depends on SA2 decisions.

Editor’s note: whether a non-3GPP device identifier needs to be reformulated into SUCI is FFS.

5. The AMF shall select an AUSF based on the received SUCI. The AMF shall send a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the non-3GPP device, the SUCI of the 5G-RG, and the SN-name. It also contains the authenticated indication generated by the W-AGF.

6. The AUSF shall send a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the non-3GPP device, the SUCI of the 5G-RG, the SN-name, and the authenticated indication.

7. The UDM shall invoke the SIDF and maps the SUCIs to the SUPIs. The UDM shall verify that the 5G-RG has been successfully authenticated and the non-3GPP device is under the control of the RG based on the subscription profiles of the 5G-RG. The UDM decides the authentication by the home network is not required for the non-3GPP device and the non-3GPP device has been authorized.

8. The UDM shall send a Nudm\_UEAuthentication\_Get Response to the AUSF. It contains the SUPI of the non-3GPP device and an indication that authentication by the home network is not required.

9. After checking the indication set by the UDM, The AUSF shall not perform authentication and shall send a Nausf\_UEAuthentication\_Authenticate Response to the AMF. It contains the SUPI of the non-3GPP device and the indication that authentication by the home network is not required set by the UDM.

This response from AUSF indicates that authentication is not required, and no KSEAF is included.

10. After checking the indication to make sure that the authentication by the home network is not required, the AMF shall estabilish the NAS security for the non-3GPP device between AMF and W-AGF with NULL encryption and NULL integrity protection.

11. The AMF shall send Registration Accept message to the W-AGF. This message contains 5G-GUTI and other parameters.

12. The W-AGF shall send a Registration Complete message back to the AMF. The W-AGF shall store the 5G-GUTI for use in later NAS procedures.

13. The W-AGF and the 5G-RG may establish a PDU session for the non-3GPP device. This is defined by CableLabs and BBF and is out the scope of 3GPP.

6.X.3 Evaluation

TBD

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