**3GPP TSG-SA3 Meeting #102 *S3-210217r1***

**e-meeting, 18-29 January 2021**

**Source: Apple**

**Title: Modification in solution#22**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to approve this solution in MEC TR 33.839.***

2 References

[1] 3GPP TR 33.839: " Study on Security Aspects of Enhancement of Support for Edge Computing in 5GC"

3 Rationale

This pCR proposes modification on solution#22 in TR 33.839.

4 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

6.22 Solution #22: Authorization during Edge Data Network change

6.22.1 Introduction

This solution addresses the security requirement for authentication/authorization during Edge Data Network change in the key issue #10.

For the Edge Data Network (EDN) change scenario, the edge service consumed by the UE will be relocated from the source EDN to the target EDN. If the secondary authentication for authorization is performed between UE and the source EDN, the issue is whether the secondary authentication between UE and target EDN is required or not. Considering the authorization requirement defined in key issue #10 and seamless change required in the key issue #2 of TR 23.748 [3], this solution gives out a simple authorization method between UE and target EDN, maintaining the seamless change requirement.

6.22.2 Solution details

 

**Figure 6.22.2-1: Authorization during the EDN relocation**

Editor’s Note: It is ffs how the T-EDN can verify a token generated by the S-EDN. The assumptions on and trust model between T-EDN and S-EDN need to be explained.

Step 1. UE sends the Registration request to the AMF and registers in the network.

Step 2. UE initiates the PDU session1 establishment procedure. It is assumed that secondary authentication is performed during the PDU session establishment procedure.

Step 3. SMF detects that EDN relocation is required and determines the T-EDN info.

NOTE 1: EDN relocation detection and T-EDN info determination will be decided in the TR 23.748 [3], and are out of scope of this document.

Step 4. SMF selects the T-UPF.

Step 5. SMF performs the N4 session configuration with the T-UPF.

Step 6. SMF sends the Authorization request to the S-EDN via S-UPF, including the GPSI, T-EDN info.

Step 7. S-EDN assures that the UE identified by the GSPI is already successfully authorized, then generates an authorization token.

Editor’s Note: Details about the token are FFS.

Step 8. S-EDN sends the Authorization response message to the SMF via S-UPF, including the token.

Step 9. If a new PDU session is required for the T-EDN, then UE initiates the PDU session2 establishment procedure for the T-EDN. Otherwise, steps 9, 13 and 14 are skipped.

NOTE X: It needs to be clarified how the PDU session2 establishment is triggered

NOTE 2: It needs to be clarified how the PDU session2 establishment is triggered. However, this is out of scope of the present document.

Step 10. SMF send the Authorization request to the T-EDN via T-UPF, including the token.

Step 11. T-EDN verifies the authorization token.

Step 12. If the authorization verification successes, T-EDN sends the Authorization response message to the SMF via T-UPF, including the success indication.

Step 13. After receiving the success indication, the SMF proceeds with the following PDU session2 establishment procedure.

Step 14. SMF sends the PDU session2 establishment response to the UE.

6.22.3 Solution Evaluation

TBD

**\*\*\*\*END OF CHANGES \*\*\***