**3GPP TSG-SA3 Meeting #102e *S3-210183***

**e-meeting, 18 – 29 January 2021**

**Source: CATT**

**Title: Remove the EN in solution #5**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***It is proposed to remove the EN in solution #5. SA3 is kindly requested to approve this contribution.***

# 2 References

[1] 3GPP TR 33.839, v0.3.0

# 3 Rationale

In the current solution#5, there is an EN on whether the secondary authentication is performed.

In the edge computing scenario, for the current Solution #5, secondary authentication will be a prerequisite for the server and the UE to supporting.

So this pCR proposes to remove the EN.

# 4 Detailed proposal

\*\*\*\*\*\* FIRST OF CHANGE \*\*\*\*\*\*\*\*\*

## 2 6.5 Solution #5: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server

### 6.5.1 Introduction

The following solution addresses the security requirement for the key issue #1 on Authentication and Authorization between the EEC and the EES.

In clause 8.3.2.3 of TS 23.558[2], before the service provisioning procedure, the Edge Enabler Client should been authorized to communicate with the Edge Configuration Server. From the security perspective, three security requirements are specified for the access of UE to Edge Data Network.

- It needs to ensure that only PLMN authorized UE can access to the Edge Data Network.

- It needs to ensure that only edge computing service authorized UE can access to the Edge Data Network.

- The URI or address information of Edge Enabler Server is the entry information for Edge Data Network when the ECS is within the MNO.

This solution proposes a mechanism to reuse the secondary authentication for the authorization of the PLMN PDU session establishment for the authentication between the EEC and the EES.

Based on the secondary authentication procedure, the client is authenticated by the EES.The SMF will allocate the Edge Applicaition Server information to the client. Then the client can use this URI information of the Edge Applicaition Server to consume the edge service.

### 6.5.2 Solution details



Figure 6.5.2-1 Authentication and Authorization between the EEC and the EES

For this solution implement, there is a prerequisite: both the UE and the EES shall support the secondary authentication.

The procedure assumes that the Edge Configuration Server is deployed by the MNO. In thi s case, the EES is the authentication server in the Edge Data Network.

1. The UE registers in the operator network and perform the primary authentication procedure. After primary authentication, the UE has the information of Edge Configuration Server.

2 When the UE triggers the edge service it sends the PDU session establishment request to the AMF to setup the PDU session for the services provided by Edge Data Network. The SMF should trigger EAP Authentication procedure and perform the role of the EAP Authenticator.

3-4. The steps 3, 4, are the same as steps 5a-5b in clause 11.1.2 of TS 33.501[7].

5. The secondary authentication procedure is required to perform if the SMF check the UE has not been authenticated and authorized by the EESThe EES is the authentication server (AAA) of the Edge Data Network.

6. This step is the same as steps 8-15 in clause 11.1.2 of TS 33.501[7].

7. After the successful completion of the secondary authentication procedure, the EES sends EAP Success message to the SMF including the registration response.

8. The SMF sends a Namf\_Communication\_N1N2MessageTransfer to the AMF with the received information.

9. The AMF forwards NAS SM PDU Session Establishment Response message along with EAP Success, and the EAS information in the registration response.

Editor's note: Whether EAS info can be acquired during the secondary authentication needs to be justified.

### 6.5.3 Solution Evaluation

TBD

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