**3GPP TSG-SA3 Meeting #103-e *S3-211708***

**e-meeting, 17- 28 May 2021**

**Source: Apple**

**Title: Evaluation on solution#8**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to add the evaluation for solution#8 in MEC TR 33.839.***

2 References

[1] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)"

3 Rationale

This pCR proposes to add the evaluation on solution#8.

4 Detailed proposal

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

6.8 Solution #8: Authentication between EEC and EES

### 6.8.1 Solution overview

This solution addresses the security requirement for the Authentication between EEC and EES in key issue #1.

In this solution, UE knows to use AKMA with EES via interact with ECS before communication with EES. If the EES deployed by MNO is considered to be trusted by the operator, the EES interacts directly with AAnF. Otherwise, the EESs not allowed by the operator to access directly the Network Functions should use the NEF to interact with AAnF.

### 6.8.2 Solution details



Figure 6.8.2-1 Authentication between the EEC and EES based AKMA

0a. UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network. If the AUSF receives the AKMA indication from the UDM, the AUSF should generate the AKMA Anchor Key (KAKMA) and the A-KID from KAUSF after the primary authentication procedure is successfully completed.

0b. After AKMA key material is generated, the AUSF should send the generated A-KID, and KAKMA to the AAnF.

1-2. The UE initiates the service provisioning procedure with the ECS. The ECS provides Edge Enabler Server Information (EES ID (i.e. FQDN or IP address(es) of EES), AKMA capability) to the UE. The AKMA capability indicates the EES support to use AKMA.

3. When the UE determines to communicate with EES, if the UE supports AKMA, the UE derives the AKMA key and the KEES(i.e. Kaf) as specified in TS 33.535 [6] based on the received AKMA capability.

4. The UE computes the MAC-I over the request message using the KEES and sending Edge Enable Client registration request with A-KID and MAC-I.

NOTE: TLS based on AKMA PSK solution is defined in other solutions.

5. Upon receiving the request, the Edge Enabler Server discovers the AAnF or NEF.

NOTE : In the case of architecture without CAPIF support, the EES is locally configured with the API termination points for the service. In the case of architecture with CAPIF support, the EES obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [9].

6. The EES contacts AAnF directly or via NEF to obtains the corresponding key KEES of the UE (as defined in TS33.535 [6])..

7. The EES verifies the MAC-I using the KEES, when the verification is succeed, and if the UE is authorized to perform the operation. The EES computes MAC-I over the response message using KECS and sends Edge Enable Client registration response with the MAC-I to the UE.

### 6.8.3 Solution evaluation

This solution doesn’t apply to the case when there are multiple EECs in one UE.

This solution requires EES to support AKMA capability.

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