**3GPP TSG-SA3 Meeting #101-e *S3-202931***

**e-meeting, 09-20 November 2020** Revision of S3-XXXX

**Source: Intel**

**Title: Authentication and Authorization Framework for EDGE-4 interfaces using Primary authentication and proxy interface**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to approve the new Solution in Edge TR 33.839.***

2 References

3 Rationale

pCR Proposes a new Authentication and Authorization Framework for EDGE-4 interfaces using Primary authentication and proxy interface.

4 Detailed proposal

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

6.Y Solution #Y: Authentication and Authorization Framework for EDGE-4 interfaces using Primary authentication and proxy interface

6.Y.1 Introduction

The solution addresses the following key issue:

• Key issue #2: Authentication and Authorization between EEC and ECS

This solution enables authentication and authorization (Proxy AA) with an ECS during registration after primary authentication successful completion. The solution is based on the KAMF generated during the primary authentication.

6.Y.2 Solution details



**Figure 6.Y.2-1: Authentication and Authorization with the Edge Data Network**

1. The UE performs normal primary authentication and registration to the network. The UE is MEC capable and may indicate this in the MEC capabilities to the AMF during the registration procedure.

2. The UE establishes a PDU Session for IP connectivity. If the UE is MEC capable, then the UE and the AMF derive a key KProxy for authentication with the ECS from the AMF key KAMF. AMF pushes the EEC ID and KProxy to the Proxy AA network function in one of the options. Proxy AA network function maintains a mapping of EEC ID and KProxy.

Editor's note: Identification of the serving AMF is FFS.

Editor’s Note: Whether the Kamf can be used to derive the Kecs in case ECS is deployed by the home network is FFS.

Editor's note: It is ffs how this solution works if the EEC ID is not unique across different UEs.

Editor's note: It is ffs how the AMF knows the EEC ID

3. The UE sends an Application Registration Request with a MAC-IProxy to the ECS. The MAC-IProxy is computed similarly as, e.g., the SoR-MAC-IAUSF, as defined in Annex A.17 of TS 33.501. The MAC-IProxy is based on the Application Registration Request's payload, which forms the input Application Registration Request Data, and the key KProxy to the KDF..

4. a. The UE is not authenticated at the ECS, and the ECS sends a Verify Request including the Application Registration Request with the MAC-IProxy to the Proxy AA through NEF, which then either verifies by retrieving context it's own stored mapping(step 2 option 1) or it sends a key request to AMF by selecting serving AMF based on UE ID the serving AMF and forwards the message to this AMF.

4. b. The AMF replies with KProxy to Proxy AA, which then stores this in its database. Proxy AA verifies the MAC-IProxy of the Application Registration Request, i.e., it computes with the key KProxy the MAC-I over the Application Registration Request payload the UE and compares the result with the MAC-IProxy included in the message. If both are identical, the message can be authenticated to be sent by the UE.

4. c. Proxy AA Devices KECS from KProxy.

4.d. The Proxy AA sends a Key Response to the ECS, including the result of the authentication and the KECS.

5. Based on the authentication result, the ECS decides whether to accept or to reject the Application Registration Request from the UE. The ECS sends the Application Registration Response message to the UE, including the authentication result, and protects the message with a MAC-IECS based on the received key KECS in a similar way as the UE protected the payload of the message.

6. The UE derives KECS from KProxy and verifies the MAC-IECS. The rest of the procedure will proceed from step 10 of solution 6.7 in 33.839.

6.Y.3 Solution Evaluation

Editor's Note: Each Solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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