**3GPP TSG-SA3 Meeting #101-e *S3-202932***

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

**Source: Intel**

**Title: Updates to Solution 4**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to approve updates to solution 4 in Edge TR 33.839.***

2 References

3 Rationale

pCR Proposes to delete the following EN in solution 4.

1: Editor’s Note: Deployment scenarios related to ECS are FFS.: Deployment scenarios are already explained in step 0 but added more details in step 0. E.g., An ECSP may have a business relationship with the operator, and UE (e.g., PC) that already has a service agreement with ECSP must use existing methodologies to connect to the ECSP to avail services.

2. Editor’s Note: Interface security for Edge-1 and Edge-4 are FFS: Added more details on for EDGE-1 and EDGE-4 interface security

4 Detailed proposal

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

6.4 Solution #4: Authentication/Authorization framework for Edge Enabler Client and Servers

6.4.1 Introduction

This solution addresses the security requirement for the Authentication and Authorization of EEC in key issue #1 and key issue #2, Key issue 4, Key issue #6(for EDGE-1, EDGE-4 interfaces). The solution should work for all the scenarios described in 23.558[2]. e.g., MNO Owned ECSP and non-MNO owned ECSP. Another scenario where the solution should be beneficial where UE already has a business relationship (e.g., subscribed to services) with ECSP and MNO has a business relationship ECSP then UE should use existing authentication/authorization methodologies to connect to ECSP to avail services.

Note: Secondary Authentication is performed in this solution.

6.4.2 Solution details



Figure 6.4.2-1: Secondary Authentication Based Authentication/Authorization framework for Edge Enabler Client and Servers

The procedure includes the following steps:

Step 0: UE pre-configuration: If the ECS deployed by MNO is contracted with one or more ECSP(s), the ECS provides EES configuration information of MNO owned, and ECSP owned EESs via MNO ECS as described in clause 8.3.3.2 in 23.558 [2]. If a non-MNO ECSP deploys the ECS, the ECS endpoint address may be configured with the EEC. An EEC that is aware of multiple ECSP's ECS endpoint addresses may perform the service provisioning procedure per ECS ECSP multiple times.

Editor’s Note: Interface security for Edge-1 and Edge-4 are FFS

Step 1: Primary Authentication: In this step, UE performs primary authentication with the network.

Step 2a, 2b: PDU session: As a result of UE initiating the service provisioning procedure with the ECS (as specified in clause 8.3 in TS 23.558 [2]), UE establishes a PDU session. This PDU Session may be established either to a well-known or pre-configured S-NSSAI or DNN, or the 5GC derives the S-NSSAI by using the registration for UE to network in step 1. Based on this information, the AMF selects an SMF, which in turn selects a PSA that provides a data connection to the Edge Cloud Service Provider's (Edge Data Network's) AAA Server. SMF continues secondary authentication as per clause 11.1.2 in 33.501[7]. ECS may act as DN-AAA Server.

Step 3a, 3b: After successful UE-requested PDU Session Establishment authentication/authorization by an EDN-AAA server, the device discovers and connects, at the application level, to a ECS server address (that was preconfigured in the UE in step 0 or is derived from the application identifier and/or Service Provider Identifier provided by the user in step 1) for provisioning EEC with ECS. The UE performs EEC registration (as specified in clause 8.4.2 in TS 23.558 [2]) and Discovery (as specified in clause 8.5 in TS 23.558 [2]) with the EES.

For authentication of the EDGE-4 reference point, mutual authentication based on client and server certificates should be performed between the Edge Configuration Server and the Edge Enabling Client, using as per clause 11.1.2 in 33.501[7].. After successfully establishing the secure session over EDGE-4 as in step 2, the Edge Enabling Client should send an Initial Provisioning request with Access Token Request message to the Edge Configuration Server as per the OAuth 2.0 specification. The Edge Configuration Server should verify the Access Token Request message per OAuth 2.0 specification. If the Edge Configuration Server successfully verifies the Access Token Request message, the Edge Configuration Server should generate an access token specific to the Edge Enabling Client and return it in an Initial Provisioning Response (Access Token Response) message.

Step 4.a: On EDGE-1, the Edge Enabling Client authenticates to the Edge Enabling Server by establishing a TLS session with the Edge Enabling Server based on the Server (Edge Enabling Server) side certificate authentication or certificate-based mutual authentication) as indicated by Edge Configuration Server. Edge Configuration Server may provide Edge Enabling Client's root CA certificate during the registration response (as specified in clause 8.4 in TS 23.558[2]) to the Edge Enabling Server to validate the Edge Enabling Client's certificate. TLS provides integrity protection, replay protection, and confidentiality protection over the EDGE-1 interface. It is required to protect and to provide the access token to an authentic EES.

Step 4.b: The UE initiates the EEC registration procedure with the EES, including the access token obtained from the ECS in Step 3.b. The authorization check for the EEC registration request is performed by verifying the access token issued by the ECS to the UE. The EES obtains the access token validation service from the ECS.

Editor’s Note: It needs to be clarified if the access token validation service by the ECS could be replaced by an authorization service by the ECS that does not require a token to be issued by the ECS to the UE

Step 5: EEC requests a service (e.g., Discovery) with access token obtained in step 4. The Edge Enabling Server should validate the access token. The Edge Enabling Server verifies the integrity of the access token by verifying the Edge Configuration Server signature. If validation of the access token is successful, the Edge Enabling Server should verify the Edge Enabling Client's Service request against the authorization claims in the access token, ensuring that the Edge Enabling Client has access permission for the requested service.

e.g., When the UE initiates the EAS discovery procedure with the EES by including the same access token obtained from the ECS in Step 3.b if it is valid. Again, the EES obtains the access token validation service from the ECS. The EES also requests and obtains the access token(s) from the ECS for the UE to grant access to the EAS(s). In response to the request, the EES includes the EAS access grant token(s), with relevant information like validity time, to the UE.

If the obtained access token from the ECS (in Step 3.b) is not valid, then the EEC requests ECS for a new access token, as shown in figure 6.3.X-1. The access token request message includes the necessary parameters to identify the EEC security context and parameters for authenticity verification. After verifying the authenticity, the ECS provides a new access token to the EEC in response to the request.

Step 6: The UE obtains service from EAS by producing the access token obtained from the EES over the secure TLS connection. The UE also obtains security policy and the relevant access token from the EES in Step 5. Before sending the access token to the EAS, the UE and the EAS establish a secure channel using the EAS server certificate. It is required to protect and to provide the access token to an authentic EAS. The EAS obtains the access token validation service from the ECS via EES. After successful validation of the access token, the UE obtains the Edge Computing service from the EAS.

6.4.3 Solution evaluation

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