**3GPP TSG-SA3 Meeting #101-e *S3-202933***

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

**Source: Intel**

**Title: Updates to Solution 12**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to approve updates to solution 12 in Edge TR 33.839.***

2 References

3 Rationale

pCR Proposes to delete the following EN in solution 12.

1)" Details of EES verification are FFS."": EN is deleted, added more clarifications in the solution.

2) "ECS certificate procedures should be FFS": Removed the text about out of the scope of 3GPP from Introduction. Add more information in step 1 as options for generating a self-signed certificate. Step 4 also mentions certificate handling.

4 Detailed proposal

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

6.12 Solution #12: Onboarding and authentication/authorization framework for Edge Enabler Server and Edge Configuration Server

6.12.1 Introduction

This solution addresses the security requirement for the Onboarding of EES with ECS, as described in Key issue 3. The solution proposes a framework and procedure that the Edge Enabling Server and the Edge Configuration Server follows to secure and authenticate the Registration, update, and deregistration of the Edge Enabling Server to the Edge Configuration Server.

As a prerequisite to this procedure (step 1), the solution assumes that Onboarding credential information is obtained by EES within the same PLMN domain or from a third party domain. EES uses onboarding credentials to authenticate and establish a secure TLS communication with the Edge Configuration Server during the registration process. The credential information includes details of the Edge Configuration Server Address and Root CA certificate, and it may also include an onboarding token (e.g., OAuth 2.0 access token). Security profiles for TLS implementation and usage shall follow the provisions given in TS 33.310 [ZZ], Annex E and F

Note: ECS address that is not belonging to the credentials, is out of scope of this document, and will be determined by SA6.

6.12.2 Solution details



Figure 6.12.2-1: Authentication/Authorization framework for EES with ECS

Step 1-2: The Edge Enabling Server and Edge Configuration Server should establish a secure session based on TLS (Server-side certificate authentication). The Edge Enabling Server should use the credential information obtained in step 1 to establish the TLS session with the Edge Configuration Server.

Editor’s Note: It needs to be clarified which credentials need to be pre-provisioned for this solution to work, and what are the trust relations between the EES, ECSP/third party and ECS.

Step 3: After the successful establishment of the TLS session, the Edge Enabling Server should send an Edge Enabler Server Registration message to the Edge Configuration Server along with the credential (OAuth access token) and EES Profile. The Edge Enabling Server generates the key pair {Private Key, Public key} and provides the public key along with the Onboard Edge Enabling Server request.

Step 4: The Edge Configuration Server should validate the enrolment credential (OAuth token). After successful verification of credentials(OAuth Token), Edge Configuration Server may generate Edge Enabling Server's certificate on its own for the assigned Edge Enabling Server identity and public key. For subsequent authentication procedures with the Edge Configuration Server, the Edge Enabling server may use this certificate to establish a secure connection and authentication with the Edge configuration Server. The Edge Configuration Server may optionally generate a Secret\_token. The Secret\_token value remains the same during the onboarding period and should be bound to the Edge Configuration Server-specific Edge Enabling Server ID. When the third party issues edge Enabling Server's client certificate, then in Step 3, the Edge Enabling Server can include the certificate in the Onboard Edge Enabling Server request message. If the Edge Configuration Server trusts the issuer of the Edge Enabling Server's client certificate, then the Edge Configuration Server includes the provided certificate in the Edge Enabling Server's profile in step 4. It is up to the Edge Computing Service Provider domain policy to accept the third party's client certificates.

Editor’s Note: optional secret\_token is FFS.

Step 5: The Edge Configuration Server should respond with a Registration response message. The response should include the Edge Configuration Server assigned Edge Enabling Server Registration ID, Edge Enabling Server Authentication and authorization information (if generated in step 4), Edge Enabling Server's certificate, and the Edge Enabling Server Secret token (if generated by the Edge Configuration Server).

6.12.3 Solution evaluation

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