**3GPP TSG-SA3 Meeting #100Bis-e *S3-202516***

**e-meeting, 12-16 October 2020**

**Source: Intel**

**Title:** **Onboarding and authentication/authorization framework for Edge Enabler Server with Edge Configuration Server**

**Document for: Approval**

**Agenda Item: 2.8**

# 1 Decision/action requested

***It is proposed to approve the Solution for Onboarding and authentication/authorization framework for Key issue 3 in TR 33.839.***

# 2 References

N/A

# 3 Rationale

# This contribution proposes the potential solution for Onboarding and authentication/authorization of the Edge Enabler Server (EES) with the Edge Configuration Server. Solution fulfils the following security requirements as stated in Key Issue 3The Edge Configuration Server and the Edge Enabling Server shall perform mutual authentication to register and update the server profile information.The Edge Configuration Server shall authorize the Edge Enabling Server to register and update the server profile information.

# 4 Detailed proposal

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

## 6.Y Solution #Y: Onboarding and authentication/authorization framework for Edge Enabler Server and Edge Configuration Server

### 6.Y.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. Procedures on how to obtain this information are out of the scope of this solution, and we believe it should be outside the scope of 3GPP. 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).

Note: ECS address that is not belonging to the credentials, may be out of SA3 scope, and will be determined by SA6.

### 6.Y.2 Solution details



Figure 6.Y.2-1: Authentication/Authorization framework for EES with ECS

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

Step 3: After the successful establishment of the TLS session, the Edge Enabling Server shall 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.

Editor Note: ECS certificate procedures shall be FFS

Step 4: The Edge Configuration Server shall validate the enrolment credential (OAuth token). After successful verification of credentials, 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..

Editor’s Note: Details of EES verification are FFS.

Step 5: The Edge Configuration Server shall respond with a Registration response message. The response shall 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 access token (if generated by the Edge Configuration Server).

6.Y.3 Solution evaluation

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