**3GPP TSG-SA3 Meeting #103-Bis-e *S3-211589-r1***

**e-meeting, 17th - 28th May 2021** Revision of S3-20xxxx

**Source: Intel**

**Title: Updates to solution 12**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***It is proposed to approve the updates to the Solution in EDGE TR 33.839.***

# 2 References

*(Reference - in list form - should be made to previous related SA5/3GPP/etc. documents.)*

*(For changes against a draft TS/TR, a pseudo CR - a.k.a. pCR - will be provided using this Tdoc template. In this case, the number, name and version of the draft TS/TR used as base must be provided and the version must be the latest available version of the draft TS/TR.)*

<Examples of references, please delete when you have inserted your actual references:

[1] 3GPP TS 32.500 SON Concepts and Requirements

[2] 3GPP TS 99.999 This example has a very long name, because then we can see how thi References paragraph will handle paragraphs spanning more than one line.

[3] 3GPP TS 99.999 Title of the document

[4] S5-991234, CR 32.999 v10.1.1, Inverting architecture of SON

[5] [S5-100001](http://www.3gpp.com/ftp/TSG_SA/WG5_TM/TSGS5_69/Docs/S5-100001.zip), Agenda, 3GPP SA5#69 Comment>

# 3 Rationale

pCR proposes to add evaluation for solution.

# 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 per 23.558[2], ECS can be owned by MNO or ECSP. ECSP can have its own authentication/authorization independent of MNO. ECSP may also have its own EES. The Edge Configuration Server(ECS) can be deployed in the MNO domain or can be deployed in 3rd party domain by the service provider in which one Edge Enabling Client may communicate with one or more Edge Configuration Server(ECS)(s) concurrently. One Edge Enabling Server may concurrently connect to one or more Edge Configuration Server with a separate EDGE-6 reference point interface. The Edge enabling server that is configured with multiple Edge Configuration Server (ECS) endpoint addresses (es) may perform the service registration, updates, or deregistration procedures per the Edge Configuration Server(ECS) of each Edge Configuration Server(ECS) multiple times. In this context, the Security Context of each of the EDGE-6 interfaces needs to be separate from each other as the trust domain may be different. In this solution, the trust relationship is based on a business relationship for each EDGE-6 interface described above.

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 [13], 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.

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. 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.

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.

6.4.3 Solution evaluation

EDGE-6 interface is protected using TLS. TLS provides integrity protection, replay protection, and confidentiality protection over the EDGE-6 interface. An O-Auth token mechanism provides authorization for EES authorization with ECS. The solution provides a mutual authentication mechanism and authorization mechanism between EES and ECS to register and update the server profile information.

With the above analysis, the solution meets the security requirements for Key issue 3.

**\*\*\*\*NEXT CHANGES \*\*\***

7 Conclusions

Editor’s Note: This clause will contain the conclusion of the TR

7.1 Conclusions for Key Issue #1

TBD.

7.2 Conclusions for Key Issue #2

TBD.

7.3 Conclusions for Key Issue #3

Solution #12 is endorsed for the normative phase for mutual authentication, authorization between Edge Configuration Server and the Edge Enabling Server to register and update the server profile information.

Note X: whether the security requirement of ECSP defined in the solution #12 is applicable depends on the definition of SA6

7.4 Conclusions for Key Issue #4

TBD.

7.5 Conclusions for Key Issue #5

TBD.

7.6 Conclusions for Key Issue #6

TBD.

7.7 Conclusions for Key Issue #7

TBD.

7.8 Conclusions for Key Issue #8

Solution #20 that was proposed to reuse the CAPIF functional security model for authentication and authorization in EES capability exposure, is endorsed for normative phase.

Editor’s Note: conclusion on the case where CAPIF is not used is FFS

7.9 Conclusions for Key Issue #9

TBD.

7.10 Conclusions for Key Issue #10

TBD.

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