**3GPP TSG-SA3 Meeting #100-e *S3-201706***

**e-meeting, 17-28 August 2020**

**Source: Intel, Samsung**

**Title: Key Issue: Security Requirements for EDGE-6 Interface**

**Document for: Approval**

**Agenda Item: 5.9**

1 Decision/action requested

***It is proposed to approve the Key Issue in TR 33.839.***

2 References

[1] 3GPP TR 23.558: "Architecture for enabling Edge Applications."

3 Rationale

TS 23.558 [1] defines the functional architecture and information flows to support Architecture for enabling Edge Applications. As per TS 23.558 [1], it is SA3 responsibility to define the security aspects of Architecture for enabling EDGE Application and for reference points Edge-1, Edge-2, Edge-3, Edge-4, Edge-5, Edge-6, Edge-7, Edge-8, Edge-9.



Figure 1- Edge Architecture

This contribution addresses the Security Requirements for EDGE-6 in SA3 Edge Security TR 33.839.

4 Detailed proposal

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

X.Y Authentication and Authorization between EES and ECS

### X.Y.1 Key Issue Details

As per 23.558[XX], the EDGE-6 reference point enables interactions between the Edge Configuration Server (ECS) and the Edge Enabler Server. EDGE-6 supported the registration and registration updates, deregistration, of Edge Enabler Server information to the Edge Enabler Network Configuration Server. The Edge Enabler Server Registration procedure allows an Edge Enabler Server to provide information to an Edge Configuration Server to request the use of its edge configuration capabilities. The Edge Enabler Server registration update procedure allows an Edge Enabler Server to update the Edge Configuration Server if there is a change in the information at the Edge Enabler Server. The Edge Enabler Server uses the Edge Enabler Server deregistration procedure to remove its information from the Edge Configuration Server. As per 23.558[XX], 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 EDGE-6 interfaces needs to be separate from each other as the trust domain may be different.

### X.Y.2 Security Threats

Without Authentication or authorization, the Malicious Edge Enabling server may be able to register with the Edge configuration server, further exposing its services to UE's Edge, enabling clients and applications running on UE.

Registration updates without any confidentiality or integrity may be able to help a Man In the middle actor impersonating the Edge configuration server to Edge Enabling server exposing and possibly altering the registration updates with falsified Edge Enabling Server profile to Edge configuration server. Also, this attack leads to exposing the topology details, server information within the PLMN domain. Malicious actors can use this exposed information for the benefit of PLMN's or Edge Computing Service provider's competitors.

### X.Y.3 Potential Security Requirements

The 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 be able to authorize the Edge Enabling Server to register and update the server profile information.

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