**3GPP TSG-SA3 Meeting #100-e *S3-201703***

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

**Source: Intel, Huawei?, HiSilicon?, Samsung?**

**Title: Key Issue: Security Requirements for EDGE-4 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-4 in SA3 Edge Security TR 33.839.

4 Detailed proposal

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

Z References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

Y Definitions, symbols and abbreviations

Y.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Y.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AC Application Client

ECS Edge Configuration Server

EEC Edge Enabler Client

EES Edge Enabler Server

FQDN Fully Qualified Domain Name

LADN Local Area Data Network

**\*\*\*\*Next CHANGES \*\*\***

X.Y Security Requirements for EDGE-4 Interface

### X.Y.1 Key Issue Details

As per [1], the EDGE-4 reference point enables interactions between the Edge Configuration Server (ECS) and the Edge Enabler Client. Edge Configuration Server (ECS) (Edge Configuration Server (ECS)) provides supporting functions needed for the Edge Enabler Client to connect with an Edge Enabler Server(EES). EDGE-4 reference point supports provisioning of Edge configuration information (e.g., URI or LADN service information) to the Edge Enabler Client.

Edge Enabler Client performs the functionalities like configuration information retrieval from the edge configuration sever over the EDGE-4 interface.

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. If the Edge Configuration Server (ECS) is deployed by MNO, the Edge Configuration Server (ECS) provides one or more Edge Enabling Server configuration information. If the Edge Configuration Server (ECS) is deployed by a non-MNO Edge computing service provider, the Edge Configuration Server(ECS) endpoint address is pre-configured with the Edge Enabling Client. The Edge enabling client that is configured with multiple Edge Configuration Server (ECS) endpoint addresses (es), may perform the service provisioning procedure per the Edge Configuration Server(ECS) of each Edge Configuration Server(ECS) multiple times. UE can contain a single Application Client (AC) or multiple Application Client(AC)s, which are served by a single Edge Configuration Server(ECS). In another scenario, UE has multiple Application Client(AC)s where each Application Client(AC) can be served by an Edge Application Server, which in turn served by a different Edge Configuration Server(ECS)'s Edge Enabling Server.

### X.Y.2 Security Threats

If access to Provisioning and configuration information is retrieved without authentication and authorization, malicious Edge enabler client will be able to receive a list of Edge Enabling Server configuration information and topology structure withing Edge Data Network from the provisioning response message. The received information can reveal Edge Data Network's topology (e.g., URI, FQDN, IP address, LADN service information, Application Server Functionalities, API type, protocols).

With different edge deployment models as described in key issue details, the Edge configuration server should be able to hide the topology and provisioning information between the trust domain of each application. Without such access control and hidden topology, Malicious application client may be able to get access to other Edge enabling servers and Edge Application servers.

Malicious Edge Enabler Client may use this information to launch attacks on Edge Data Network or use this information for competitive reasons.

### X.Y.3 Potential Security Requirements

Edge Configuration Server(ECS) Requirements:

Edge Configuration Server(ECS) shall be able to provide mutual authentication with Edge Enabler Client over EDGE-4 Interface.

Edge Configuration Server(ECS) shall be able to determine whether Edge Enabling the client is authorized to access provisioning services offered by Edge Configuration Server(ECS).

Edge configuration server shall be able to hide topology details between the trust domains of each application client.

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