**3GPP TSG-SA3 Meeting #105-e *S3-*** ***214270***

e-meeting, 8 - 19 November 2021Revision of S3-20xxxx

**Source: Ericsson**

**Title: Updates to KI#1 and KI#2**

**Document for: Approval**

**Agenda Item: 5.6**

# 1 Decision/action requested

***Approve the proposed pCR to TR 33.839.***

# 2 References

[1] 3GPP TR 33.839 "Study on security aspects of enhancement of support for edge computing in 5G Core (5GC)"

# 3 Rationale

Main security threat stated in KI#1 and KI#2 in TR 33.839 [1] is that an unauthorized client can learn topology structure within Edge Data Network from the servers. As discussed in SA3#104e-Adhoc meeting, there is another threat which can be more serious than the leaking topology information. We can call this new threat as a privacy threat where a malicious client and UE can learn some information about location of victim subscribers. Some of possible attacks are as follows:

* Assume that the attacker knows the topology in advance. He/she can send the GPSI of the victim UE to the server (EES/ECS). The server learns the location of the UE from the 3GPP network, prepares a list of servers considering this location information, and sends this list to the attacker. Using the location dependent list, the attacker may learn some information about the location of UE, for example the attacker can check whether the victim UE is in a specific city.
* Assume that the attacker doesn’t know the topology. If the attacker and the victim UE are subscribers of the same edge application, then the attacker first learns the list of servers for itself and then learns the list of servers for the victim UE. If the server lists match, then it means that the attacker and the victim UE is in the same location/area/city.

To prevent such privacy attacks, it is important to authenticate the GPSI so that no one can send the GPSI of other UEs to the server.

Also, it may be important to authenticate applications, running of the UE, which try to get services from the server because a malicious application, which is not authorized to learn the location of the UE, running on the UE can learn some information about the UE because of the services provided by the servers. In this case, authentication of GPSI may not be enough because the malicious application runs on the same UE. Note that to prevent such an attack, it is not necessary to authenticate the instance id of the EEC. Validation of that the EEC is a legitimate application can be enough. In addition, the validation of the EEC type can bring value in terms of security. With the validation of the EEC type, the server can prepare the list of servers considering the type of the EEC. EEC type can be regarded as application type/id.

With this motivation, this contribution proposes some updates to KI#1 and KI#2 to address the privacy attack and put some related security requirements.

# 4 Detailed proposal

#### \*\*\* Start of 1st Change \*\*\*

## 5.1 Key issue #1: Authentication and Authorization between EEC and EES

### 5.1.1 Key Issue Details

As per TR 23.558 [2], EDGE-1 reference point enables interactions between the Edge Enabler Server and the Edge Enabler Client. EDGE-1 reference point supports registration and de-registration of the Edge Enabler Client to the Edge Enabler Server, retrieval and provisioning of Edge Application Server configuration information; and discovery of Edge Application Servers available in the Edge Data Network.

Edge Enabler server provides functionalities to Edge Enabler client over EDGE-1 reference point such as provisioning of configuration information to Edge Enabler Client and support the functionalities of application context transfer.

Edge Enabler Client performs the functionalities like configuration information retrieval from the edge enabler server and discovering of the edge application servers available in Edge Data Network. The Edge Data Network is a local Data Network. Edge Application Server(s) and the Edge Enabler Server are contained within the EDN.

The UE is initially provisioned with the configurations required to connect to the Edge Data Network. Upon initial provisioning, the Edge Enabler Client of the UE registers with the selected Edge Enabler Server(s) from the list of provisioned Edge Enabler Server(s). Edge Enabler Client consumes service offered by the Edge Enabler Server, e.g. discovering Edge Application Servers in an area of interest. The procedure enables the initialization or update of the Edge Enabler Client context information at the Edge Enabler Server. The Edge Enabler Client sends the Edge Enabler Client registration request to the Edge Enabler Server. Edge Application Server discovery enables Edge Enabler Clients to obtain information about available Edge Application Servers of interest. The identification of the Edge Application Servers is based on matching query filters or Application Client Profiles provided in the request.

GPSI can be used as a UE identifier inside and outside of 5G networks, as specified in TS 23.501[14] and TS 23.003[15]. As specified in TS 23.558[2], a new edge enabler layer is defined. In order to identify the UE's Edge Enabler Client, the UE uses Edge Enabler client ID as the client identifier at the edge enabler layer. And the Edge Enabler client ID may be used along with GPSI. Then the EEC uses two different identifiers towards the EES, EEC ID and UE identifier (could be GPSI)). Solutions to this key issue need to clearly state which identifier of the EEC they authenticate.

Editor's Note: It is FFS whether the EEC ID will be unique across different UEs.

Editor’s Note: Whether the binding issue between EEC ID and UE identifier is required is FFS.

### 5.1.2 Security Threats

When Registration, Discovery , Deregistration is used without authorization, malicious Edge enabler client receives a list of Services and topology structure within Edge Data Network from Edge Enabler Server discovery response message. The received information can reveal Edge Data Network’s topology (e.g. URI, IP address, number of Edge Application Servers, Application Server Functionalities, API type, protocols). Malicious Edge Enabler Client may use this information to launch attacks on Edge Data Network or use this information for competitive reasons.

If GPSI is not authenticated, then a malicious application that spoofs a victim UE’s GPSI can learn some information about the location of the victim UE’s location because the edge application server lists returned to the application is constructed considering the UE location learned from the 3GPP network.

If the EEC, an application running on the UE, is not authenticated, then a malicious application, running on the victim UE, that is not authorized to learn the location of the UE will be able to learn some information about the UE location because of the reason explained above.

### 5.1.3 Potential Security Requirements

Edge Enabler Server shall be able to provide mutual authentication with Edge Enabler Client over EDGE-1 Interface.

Edge Enabler Server shall be able to determine whether Edge Enabling client is authorized to access Edge Enabling Server’s services.

Edge Enabler Server shall be able to authenticate the GPSI sent by the Edge Enabler Client if the client sends the GPSI to the server.

\*\*\* End of 1st Change \*\*\*

#### \*\*\* Start of 2nd Change \*\*\*

## 5.2. Key issue #2: Authentication and Authorization between EEC and ECS

### 5.2.1 Key Issue Details

As per TR 23.558[2], 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 TR 23.558[2], 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 is served by a different Edge Configuration Server(ECS)'s Edge Enabling Server.

GPSI can be used as a UE identifier inside and outside of 5G networks, as specified in TS 23.501[14] and TS 23.003[15]. As specified in TS 23.558[2], a new edge enabler layer is defined. In order to identify the UE's Edge Enabler Client, the UE uses Edge Enabler client ID as the client identifier at the edge enabler layer. And the Edge Enabler client ID may be used along with GPSI. Then the EEC uses two different identifiers towards the EES, EEC ID and UE identifier (could be GPSI)). Solutions to this key issue need to clearly state which identifier of the EEC they authenticate.

Editor's Note: It is FFS whether the EEC ID will be unique across different UEs.

Editor’s Note: Whether the binding issue between EEC ID and UE identifier is required is FFS.

### 5.2.2 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 within 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).

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

If GPSI is not authenticated, then a malicious application that spoofs a victim UE’s GPSI can learn some information about the location of the victim UE’s location because the edge enabler server lists returned to the application is constructed considering the UE location learned from the 3GPP network.

If the EEC, an application running on the UE, is not authenticated, then a malicious application, running on the victim UE, that is not authorized to learn the location of the UE will be able to learn some information about the UE location because of the reason explained above.

### 5.2.3 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 authenticate the GPSI sent by the Edge Enabler Client if the client sends the GPSI to the server.

\*\*\* End of 2nd Change \*\*\*