**3GPP TSG-SA3 Meeting #102-e *S3-210171-r1***

**e-meeting, 18 - 29 January 2021** Revision of S3-21XXXX

**Source: ZTE Corporation**

**Title: LBO roaming scenario should be supported in solution#6.7 in TR 33.839**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***This contribution proposes to add the roaming scenario to the solution# 6.7.***

# 2 References

*(Reference - in list form - should be made to previous related SA3/3GPP/etc. documents.)*

[1] 3GPP TR 33.839 V0.3.0“Study on Security Aspects of Enhancement of Support for Edge Computing in 5GC”.

[2] 3GPP TS 23.501 V16.7.0“System architecture for the 5G System (5GS)”.

# 3 Rationale

In last SA2 meeting, it has mentioned in the clause 5.13 of the TS 23.501[2] that edge computing supports roaming scenarios, as follows:

## *5.13 Support for Edge Computing*

*Edge computing enables operator and 3rd party services to be hosted close to the UE's access point of attachment, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.*

*NOTE: Edge Computing typically applies to non-roaming and LBO roaming scenarios.*

*The 5G Core Network selects a UPF close to the UE and executes the traffic steering from the UPF to the local Data Network via a N6 interface. This may be based on the UE's subscription data, UE location, the information from Application Function (AF) as defined in clause 5.6.7, policy or other related traffic rules.*

This contribution proposes to add the roaming scenario to the solution#6.7 in TR 33.839[1].

# 4 Detailed proposal

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

## 6.7 Solution #7: Authentication and Authorization with the Edge Data Network

### 6.7.1 Solution overview

The solution addresses the following key issues:

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

- Key issue #2: Authentication and Authorization between EEC and ECS

- Key issue #6: Transport security for the EDGE-1-9 interfaces

The solution is based on the KAMF generated during the primary authentication. The network function that receives a registration request is querying the previous network function for authentication and the key for setting up an IPsec SA. Messages are protected with a MAC-I, which is also used to authenticate the UE.

The preferred ECS deployment scenario of the solution is, when the ECS is located in the serving network or hosted by a 3rd party service provider, since the services are to be hosted close to the UE's access point of attachment, to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network. In case of special roaming scenarios where the ECS is only located in the HPLMN while the UE is in a VPLMN, the KECS is then derived from the VPLMN KAMF.

NOTE: Edge Computing typically applies to non-roaming and LBO roaming scenarios.

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