**3GPP TSG-SA3 Meeting #102-e *S3-210173-r1***

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

**Source: ZTE Corporation**

**Title: Update the solution #14 in TR 33.839**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***This contribution proposes to update the solution #14 in TR 33.839.***

# 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 23.748 V17.0.0“Study on enhancement of support for Edge Computing in 5G Core network (5GC)”.

# 3 Rationale

In last SA2 meeting, it has drawn some conclusion for key issue #3 in the TS 23.748[2]:

*The following principles abstracted from solutions #43, #46, #48, and #49 are recommended as the baseline for normative work:*

*1. Local PSA UPF generated QoS monitoring results based on RAN reporting via GTP-U packets as defined in TS 23.501 [2], clause 5.33.3.*

*2. The AF subscribes low latency exposure of QoS monitoring results via Local NEF/NEF and PCF.*

*3. Local PSA UPF exposes the QoS monitoring results to local AF via local NEF.*

*4. The address of the local NEF may be obtain using NRF-based discovery procedures.*

*NOTE 1: Local PSA UPF can expose the QoS monitoring results to local AF via N6. How to deliver the information on N6 is out of scope.*

*NOTE 2: Exposure for edge computing applications can be supported with a (potentially locally) deployed NEF/SMF and existing interface for exposing Notification Control and QoS monitoring, in the case the SMF can be locally deployed and the added latency by the SMF and the extra routing path does not make the overall exposure latency exceed the required exposure latency.*

*NOTE 3: Sending QoS monitoring information that has not been properly integrated over time incurs the risk that the application may over-react to instantaneous radio events/conditions leading to service instability*.

Therefore, there is no new interface between the UPF and the local AF and how to deliver the information on N6 is out of scope.

# 4 Detailed proposal

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

## 6.14 Solution #14: Protection of Network Information Provisioning to Local AF directly

### 6.14.1 Solution overview

This solution addresses the security requirement for the case that the UPF exposes information to local AF directly in the key issue 7.

NOTE: The interface between local UPF and local AF is N6 and how to deliver the information on N6 is out of scope.

### 6.14.2 Solution details



Figure 6.14.2-1 Protection of Network Information Provisioning to Local AF

1. AF establish a TLS session with the NEF, to secure the communication between the AF and NEF.

2a-2b. The AF generates a Key-ID for the UE and derives a KLE. The Key-ID is used to identify the KLE, and the KLE is used to protect the message transmission between UPF and AF. The AF provides the Key-ID to NEF in the request service.

3-4. The NEF initiates the policy authorization with PCF, including the K-ID and KLE received from the AF. PCF initiates the PDU session modification procedure as defined in clause 4.3.3.2 of TS 23.502 [3] and provides the Key-ID and KLE to the SMF.

5. SMF sends the notification information with Key-ID and KLE to the UPF.

6. When the QoS monitoring information is received from RAN, the UPF generates MAC-I over the message using the KLE to prove its authenticity. The UPF sends the message including Key-ID and MAC-I to AF.

7. The AF retrieves the KLE based on the received Key-ID and verify the MAC-I.

### 6.14.3 Solution evaluation

TBD.

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