**3GPP TSG-SA3 Meeting #102-e *S3-210172-r1***

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

**Source: ZTE Corporation**

**Title: Update the key issue#7 in TR 33.839**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***This contribution proposes to update the key issue#7 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 \*\*\*\****

## 5.7 Key Issue #7: Security of Network Information Provisioning to Local Applications with low latency procedure

### 5.7.1 Key issue details

In the solutions for network information provisioning to local application procedure in TR 23.748 [3], the following two ways are proposed to perform network information exposure to local application.

- UPF exposes the network information (i.e. QoS monitoring) to local AF via Local NEF.

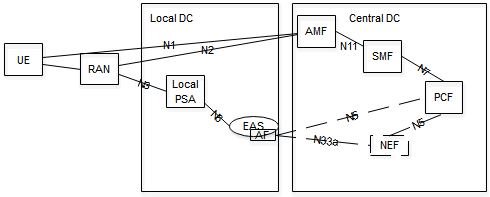


For this case, the following two alternatives proposed:

- The EAS/AF subscribes the network information notification according to the blue dashed line path, and the local PSA provisions the networking information to EAS/AF via local NEF (i.e. according to the blue solid line path).

- The EAS/AF subscribes the network information notification according to the red dashed line path, in this case, the local NEF retrieves the UPF information before subscribing the event from UPF for AF which is not showed in the figure. When the request event happens, the local PSA provisions the networking information also to EAS/AF via local NEF (i.e. according to the blue solid line path).

- UPF exposes the network information to local AF directly.



For this case, the following two alternatives proposed:

- The EAS/AF subscribes the network information notification according to the blue dashed line path, and the local PSA provisions the networking information to EAS/AF directly (i.e. according to the blue solid line path).

- The EAS/AF subscribes the network information notification with UPF directly (i.e. according to the red dashed line path).

New interface between UPF and local NEF/EAS was introduced, we need to study the security issue on the new interface.

NOTE: 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.

### 5.7.2 Security threats

Without authentication and protection, an attacker may eavesdrop or manipulate or replay the communication on the new interface.

### 5.7.3 Potential Security requirements

For the case that UPF exposes the network information to local AF via Local NEF.

* Mutual authentication mechanism between UPF and local NEF shall be supported.
* Confidentiality protection, integrity protection and replay-protection shall be supported on the new interface between UPF and local NEF.

For the case that UPF exposes the network information to local AF directly:

* The UPF enable secure provision of information in the 3GPP network by authenticated and authorized Application Functions.

Confidentiality protection, integrity protection and replay-protection shall be supported on the interface between UPF and Application Functions.

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