**3GPP TSG-SA3 Meeting #105-e *draft\_S3-214141-r1***

**e-meeting, 8 - 19 November 2021** Revision of S3-21xxxx

**Source: Qualcomm Incorporated, CATT**

**Title: Additional conclusion of KI #17 – UP security policy**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

***This contribution proposes a conclusion of KI #17***

# 2 References

[1] TR 33.847 v0.8.0

[2] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services"

# 3 Rationale

When user-plane solutions are used for the PC5 security, it was concluded that the PKMF provisions the security materials at the UEs (see 7.3 of TS 33.847 [1], i.e., conclusion of KI #3). Since the PKMF is the anchor of the PC5 security for the user-plane solutions, it is proposed to conclude that when user-plane solutions are used for PC5 security, the security policies for the PC5 are also provisioned by the PKMF along with the PC5 security materials. With this approach, there is a single entity that manages the security of the PC5 link, which can eliminate potential misconfiguration/inconsistency of security materials and/or policies at the network. Furthermore, the PKMF may cross-check the UP policies for a relay service (identified by RSC) during the interactions with PKMFs in other PLMNs (e.g., in roaming scenarios).

Since emergency services via U2N relay is not supported in Rel-17 according to SA2, it is proposed to make the signaling integrity protection mandatory for U2N relay. This should be implemented by setting the signaling integrity protection policy to “REQUIRED”. For other one-to-one communications, it is proposed to determine the signaling integrity protection based on the signaling security policy as defined in TS 33.536 [2] to cover various use cases.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [1].

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

## 7.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services

* The following text is taken as conclusions for the security policy handling:Security policy provisioning:
  + For user-plane UE-to-network relay solutions, the PKMF provides the security policies to the UE.

NOTE: PKMF may get the security policies in different ways (e.g., from PCF, from ProSe Application server, or based on local configuration) and this will be decided in the normative phase.

* + For control-plane UE-to-network relay solutions, the PCF provides PC5 security policies to the UE as per TS 33.356 [8].
* The security policy negotiation and enforcement for PC5 connection is based on the TS 33.536 [8].
* The security policy for signaling integrity protection on PC5 is set to “REQUIRED” for all UE-to-network relay scenarios.

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