**3GPP TSG-SA3 Meeting #116 *S3-242048-r1***

Jeju, South Korea, 20th - 24th May 2024

**Title: Reply LS on the use of TLS with QUIC in ATSSS context**

**Response to: LS <S2-2405459> on the use of TLS with QUIC in ATSSS context from SA2**

**Release: release 18**

**Work Item: ATSSS\_Ph3**

**Source: Intel (to be SA3)**

**To:** **SA WG2**

**Cc:**

**Contact person: Abhijeet Kolekar**

**Abhijeet.kolekar@intel.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:** S3-24bbbb

# 1 Overall description

SA3 thanks SA2 for the LS (S2-2405459) regarding the Editor’s note on using TLS with QUIC in clause 5.32.6.2.2 of TS 23.501. SA3 proposes to delete the Editor’s Note related to MPQUIC. Also, SA3 would like to notify that

For Rel-18, SA3 endorses using digital certificates provisioned in the UPF to facilitate server authentication by the UE. In this case, when using TLS as part of QUIC, at least one-way authentication (i.e., UE authenticating the UPF) needs to be performed. This implies provisioning a digital certificate in the UPF and root of trust in the UE.SA3 asks SA2 to propose the following note by deleting the Editor’s Note related to MPQUIC

“NOTE: Regarding the provisioning of certificates, the root of trust in the UE, and ~~related to~~ UPF ~~server~~ mutual authentication is left to the implementation. “

“NOTE: Exposing the UPF IP addresses to the UE is against the principle of network topology hiding. It is up to the network to decide to compromise on the security to use MPQUIC.”

# 2 Actions

**To SA2**

**ACTION:** SA3 kindly asks SA2 to take into consideration the above information.

# 3 Dates of next TSG SA WG 3 meetings

SA3#117 19 - 23 August 2024 Maastricht (Netherlands)

SA3#118 14 - 18 October 2024 Hyderabad (India)