**3GPP TSG-SA3 Meeting #124 S3-253387**

**Wuhan, China, 13 – 17 October 2025**

**Source: Huawei, HiSilicon**

**Title: New solution of using pre-configured PSK to establish the security of MPQUIC**

**Document for: Approval**

**Agenda item: 5.2.5**

**Spec: 3GPP TR 33.778**

**Version: 0.0.0**

**Work Item: FS\_PSK\_MQC\_TLS**

**Comments**

As we know, hop-by-hop security mechanism has already been provided for UE and UPF data transmission. For ATSSS scenario, other high layer steering functionalities (e.g. MPTCP, ATSSS-LL) than MPQUIC do not have additional security features. From this point of view, this high-level intergrated TLS security is not essential, and the overhead of this function can be minimized. From this point of view, it is proposed to use a pre-configured key to establish the security of MPQUCI between UE and UPF supporting MPQUIC functionalities.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

…

[x] 3GPP TS 23.502: "Procedures for the 5G System".

[y] IETF RFC 9001: " Using TLS to Secure QUIC".

[z] IETF draft-ietf-quic-multipath: "Multipath Extension for QUIC".

\* \* \* Second Change \* \* \* \*

## 6.Y Solution #Y: Using pre-configured PSK to establish the security of MPQUIC

### 6.Y.1 Introduction

This solution addresses key issue #X “PSK support for MPQUIC TLS”.

This solution proposes to use a pre-configured key to establish the security of MPQUIC for UE and UPF supporting MPQUIC functionality.

### 6.Y.2 Solution details

The pre-shared key and the identifier of this pre-shared key can be pre-configured to the UE and UPF supporting MPQUIC functionalities by out of band means. The pre-configured PSK for UPFs in the same PLMN can be the same or different, which is determined by the operator.

The MA PDU session establishment procedure can be referred to the 3GPP TS 23.502 [x]. After the establishment of the UE's MA PDU session is completed, the UE and the selected UPF negotiate to establish an MPQUIC connection, which is associated with the MA PDU session.

Since both the UE and UPF store the same pre-configured key and the identifier of this pre-configured key. When the UE and UPF negotiate to establish the MPQUIC connection, the UE sends the identifier of the pre-configured key to the UPF. Correspondingly, the UPF determines the pre-configured key based on the identifier of the pre-configured key, and then, if it agrees to use the pre-configured key to establish an MPQUIC connection with the UE, it sends the identifier of the pre-configured key to the UE. In this way, both parties agree on the key (i.e., the pre-configured key) to be used for establishing the MPQUIC connection. The subsequent process of establishing security using this pre-configure key can be referred to [y][z].

### 6.Y.3 Evaluation

This solution provides a method for establishing MPQUIC with pre-configured shared keys. As described above, this solution requires pre-configuring the same key for the UE and UPF through out-of-band means. Consequently, there may be a certain burden on UEs and UPFs that support MPQUIC functionality. Editor’s Note: Further evaluation is FFS.

\* \* \* End of Change \* \* \* \*