**3GPP TSG-SA3 Meeting #124 draft\_S3-253712-r2**

**Wuhan, China, 13 – 17 October 2025** revision of S3-253292

**Source: Interdigital**

**Title: New Solution for MPQUIC/TLS using PSK derived from KgNB**

**Document for: Approval**

**Agenda item: 5.2.5**

**Spec: TR 33.778**

**Version: 0.0.0**

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

**Comments**

It is proposed to add this new solution for the support for MPQUIC/TLS using PSK, between UE and UPF.

\* \* \* First Change (all text new)\* \* \* \*

## 6.X Solution #X: MPQUIC/TLS using PSK derived from KgNB

### 6.X.1 Introduction

This solution addresses Key issue #1 by enabling a secure UP communication channel between the UE and the UPF. The approach leverages the current KgNB to derive a pre-shared key (UPF\_PSK) and a corresponding identifier (UPF\_PSK ID). The UPF\_PSK/ID is delivered to the UPF and then used for a mutual-authentication and key exchange using TLS 1.3 PSK psk\_dhe\_ke.

### 6.X.2 Solution details

**Assumptions and scope:**

 - UE is registered to the 5GS and has established a KgNB with the network.

 - Distribution path for UPF\_PSK/ID: AMF/SMF → UPF over N2/N4.

**Key derivation and identifiers:**

**-** UE and AMF derive UPF\_PSK and UPF\_PSK ID using current KgNB.

- Input parameters for the KDF include at least the PDU Session ID and a freshness parameter. UPF\_PSK derivation can additionally be bound to the selected UPF identity (e.g., FQDN or IP).

Editor’s Note: Motivation for derivation of UPF\_PSK using KgNB is FFS.

**Setup procedure (PDU Session establishment):**

- UE requests a PDU Session indicating support for MPQUIC/TLS using PSK.

- SMF selects a suitable UPF and provides UE with UPF addressing (e.g., IP, port) and obtains UPF\_PSK/ID from AMF.

- AMF derives UPF\_PSK/ID from current KgNB. SMF forwards UPF\_PSK/ID to UPF via N4.

- Upon successful PDU Session Establishment, UE initiates MPQUIC/TLS with the UPF using UPF\_PSK, referencing UPF\_PSK ID for UPF to locate and use UPF\_PSK to perform mutual authentication with the UE.

**UPF\_PSK update triggers and handling:**

- UE CM-IDLE → CM-CONNECTED transition:

- UE and AMF derive new UPF\_PSK/ID.

- AMF/SMF updates the UPF with the new UPF\_PSK.

- UE initiates MPQUIC/TLS with the UPF using the new UPF\_PSK/ID.

Editor’s Note: applicability of the update trigger condition is FFS.

### 6.X.3 Evaluation

Editor’s Note: Evaluation is FFS