**3GPP TSG-SA3 Meeting #124 draft S3-253718-r1**

**Wuhan, China, 13 – 17 October 2025 revision of S3-252563**

**Source: Nokia**

**Title: Solution on leveraging PSK for MPQUIC TLS**

**Document for: Approval**

**Agenda item: 5.2.5**

**Spec: 3GPP TR 33.778**

**Version: 0.0.1**

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

**Comments**

During SA3#123 meeting the new Study on MPQUIC was approved (S3-252961) with the following objectives:

Based on the above justification, the following objectives will be studied:

WT#1: Study the support of PSK mode, in particular:

- Study key derivation and delivery for UPF.

NOTE: the impact to the 5GS should be minimized.

The following solution is proposed to address both key derivation and delivery aspects.

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

6.Y Solution #Y: Key derivation and delivery to UE and UPF

6.Y.1 Introduction

The following solutions addresses KI#1 by proposing a mechanism to derive the key inside the 5G core and distribute it to both UE and UPF. Additionally, it proposes a mechanism to initiate re-authentication by deriving and delivering new keys to UE and UPF.

6.Y.2 Solution details

#### 6.Y.2.1 Key derivation and distribution



1. A Multi-Access PDU session is established and one or more ATSSS rules require the use of MPQUIC.

2. The UPF request SMF the pre-shared secret for the session with the UE.

3. SMF forwards the Key request to AMF.

4. AMF generates the new key by deriving it from KAMF. The following parameters should be use as input to the KDF:

- FC= 0xWX

- P0= Random Number

- L0= P0 length

5.a. AMF sends a response to SMF containing the generated key.

5.b. AMF send the key and PDU session ID to UE to identify where the correct session to use the key.

6. SMF forwards the response, along with the Key and an identifier of the UE to UPF.

7. UE and UPF authenticate each other and initiate the MPQUIC connection as supported in ATSSS based on the pre-shared secret, i.e., the key.

Editor’s Note: Key derivation and delivery from serving network to home network in roaming scenarios is FFS.

#### 6.Y.2.2 Re-Keying mechanism



1. MPQUIC connection has been set up through PSK.

2. Either UE or 5G core requires to renew the pre-shared secret.

3. AMF generates a new key through the same mechanism used during the initial key derivation.

4.a. AMF sends notification of the new Key to UE.

4.b. AMF replies to SMF with the new key.

5. SMF provides the new key to UPF.

6. UE and UPF gracefully terminate the current MPQUIC session.

7. UE and UPF establish a new one based on the pre-shared key.

Editor’s Note: Key update for reauthentication is FFS.

Editor’s Note: The need for a key renewal is FFS.

6.Y.3 Evaluation

The solution completely addresses the problem highlighted by KI#1 both for initial authentication of the connection and for update of the key in case of a compromise. The security is achieved by deriving a new dedicated key for each MPQUIC connection, ensuring that each connection is independently secured, and the compromise of one key will not impact the security of the overall system.

The solution impacts AMF by enhancing its key derivation capabilities to support the new use case. Additionally, it defines delivery mechanism which impact SMF, as both initiator of the procedure and intermediate layer between AMF and UPF, and UPF in the 5G core and the connection towards the UE.

The solution relies on AS security to ensure the confidentiality of the PSK, deactivating the AS security will impact the security of the solution.

Editor’s Note: Further eval is FFS.

\* \* \* End of Changes \* \* \* \*