**3GPP TSG-SA3 Meeting #124 draft\_S3-253714-r1**

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

**Source: Xiaomi, Samsung ?**

**Title: Solution for PSK Delivery**

**Document for: Approval**

**Agenda item: 5.2.5**

**Spec: 3GPP TR 33.778**

**Version: 0.0.0**

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

**Comments**

This pCR proposes a new solution for delivering the PSK to the UPF, which is used to enable MPQUIC/TLS in ATSSS scenario.

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

## 6.Y Solution #Y: PSK delivery during MA PDU session establishment

### 6.Y.1 Introduction

According to TS 23.502 [x] clause 4.22.2, when receiving the UE requested PDU session establishment request with Request Type as "MA PDU Request", the AMF supporting MA PDU sessions selects an SMF supporting MA PDU sessions. It is proposed that:

- When selecting an SMF supporting MA PDU, the AMF sends a key to the SMF for PSK derivation.

The SMF determines to use MPQUIC for the new PDU session based on TS 23.502 [x] clause 4.22.2, then selects and configures the selected UPF supporting MPQUIC. It is proposed that:

- When determining that MPQUIC is to be used for the PDU session, the SMF derives the PSK;

- When configuring the UPF, the SMF provides the derived PSK to the UPF.

On the UE side, when the UE receives a PDU Session Establishment Accept message indicating that the requested MA PDU session was successfully established, the message will include the ATSSS rules for the MA PDU session derived by SMF. If MPQUIC functionality is supported for the MA PDU Session, the SMF will include the "MPQUIC link-specific multipath" addresses/prefixes of the UE and the MPQUIC proxy information that corresponds to the activated MPQUIC-based steering functionality in the ATSSS rules. It is proposed that:

- The UE derives the PSK when receiving the ATSSS rules from the SMF containing the "MPQUIC link-specific multipath" addresses/prefixes of the UE and the MPQUIC proxy information.

- The UE then uses the derived PSK to authenticate with the UPF using MPQUIC/TLS protocol.

### 6.Y.2 Solution details

The detailed procedure is shown in Figure 6.Y.2-a.



Figure 6.Y.2-a: MPQUIC/TLS Security Establishment during MA PDU session establishment

1. The UE provides Request Type as "MA PDU Request" in UL NAS Transport message and its ATSSS capabilities in PDU Session Establishment Request message.

2. Based on Request Type as "MA PDU Request" received from the UE, if the AMF supports MA PDU sessions, the AMF selects an SMF which supports MA PDU sessions. The AMF informs the SMF that the request is for a MA PDU Session by including "MA PDU Request" indication.

In addition, the AMF may send a derived PSK to the SMF or send a root key to the SMF for PSK derivation.

The root key could be the KAMF or KSEAF or KSMF derived from KAMF or KSEAF.

3. The SMF retrieves, via Session Management subscription data, the information whether the MA PDU session is allowed or not.

4. The SMF returns a Nsmf\_PDUSession\_CreateSMContext Response to the AMF.

5. The SMF determines the ATSSS capabilities supported for the MA PDU Session taking into consideration the ATSSS capabilities provided by the UE and per DNN configuration on SMF. The SMF initiates an N4 Session Establishment/Modification procedure with the selected UPF. If the MPQUIC functionalities are supported for the MA PDU Session, the SMF instructs the UPF to activate the corresponding functionalities for this MA PDU Session. The SMF receives the UE IP address of the MA PDU session from the UPF.

6. Upon receiving a positive N4 Session Establishment/Modification Response, the SMF derives the PSK from the root key if received from the AMF.

Alternatively, the SMF can also decide to derive the PSK at step #12 after receiving positive PDU session response from the AMF.

If the AMF does not send a root key in step #2, the SMF sends a key request to the AMF/SEAF to acquire the PSK derived by the AMF/SEAF or retrieve the root key before deriving the PSK.

The PSK derivation refers to solution #X.

7. The SMF sends the Namf\_Communication\_N1N2MessageTransfer message to the AMF.

8. The AMF sends the PDU Session Request message to the gNB.

9. The gNB issues AN specific signalling exchange with the UE that is related with the NAS information received from SMF.

10a. Upon receiving the ATSSS rule in the NAS message from the AMF, if ATSSS rule contains the "MPQUIC link-specific multipath" addresses/prefixes of the UE and the MPQUIC proxy information, the UE determines to derive the PSK from the root key in the same way as the AMF or SMF.

10b. After AN specific signalling exchange with the UE, the gNB returns the PDU Session Response message to the AMF.

11. The AMF sends the Nsmf\_PDUSession\_UpdateSMContext Request to forward the N2 SM information received from gNB to the SMF.

12. The SMF derives the PSK if not received in step #2 or not derived in step #6.

13. The SMF sends the PSK to the UPF in the N4 Session Modification Request.

14. The UE and UPF perform authenticate using MPQUIC/TLS based on the PSK, then negotiate and establish TLS tunnel security.

15. The UPF returns the N4 Session Modification Response to the SMF.

16~17. From this step onwards, the TLS security between the UE and UPF is established for protecting user plane traffic between the UE and the UPF.

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

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

### 6.Y.3 Evaluation

Editor’s Note: This clause is going to capture the pros and cons of the solution, e.g. whether the threats are addressed totally, how the existing 5G system is impacted, whether there is any leftover issues exists, etc.

\* \* \* Next 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 (5GS)".

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