**3GPP TSG-SA3 Meeting #124 draft\_S3-253713-r1**

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

**Source: Xiaomi**

**Title: Solution for PSK Derivation**

**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 derivation of the PSK used to enable MPQUIC/TLS in ATSSS scenario.

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

## 6.Y Solution #Y: PSK derivation bound with MA PDU session

### 6.Y.1 Introduction

According to TS 23.501 [x] clause 5.32.6, for steering functionalities based on MPQUIC that apply the QUIC protocol and its multipath extensions, the MPQUIC functionality(ies) in the UE communicates with the associated MPQUIC Proxy functionality(ies) in the UPF. The MPQUIC functionality in the UE and the associated MPQUIC Proxy functionality in the UPF uses the "MPQUIC link-specific multipath" addresses/prefixes for transmitting traffic flows over non-3GPP access and over 3GPP access. The "MPQUIC link-specific multipath" IP addresses/prefixes are allocated by the UPF and provided to the UE via SM NAS signalling. For multiple paths sharing the same TLS tunnel, it is proposed that:

- On the UE side, the PSK is derived by the UE and used by the MPQUIC functionality in the UE.

- On the network side, the PSK is used by the associated MPQUIC Proxy functionality in the UPF. The PSK is derived by the SMF or the AMF which holds the root key for PSK derivation and the derived PSK is delivered to the UPF.

- The PSK is bound with a specific MA PDU session, in which way the old PSK used on authentication for an existing MA PDU session cannot be reused on authentication for a new MA PDU session.

### 6.Y.2 Solution details

To bound the PSK with a specific MA PDU session, it is proposed to use an identity which can uniquely identify the MA PDU session on both the UE side and network side as an input parameter for PSK derivation. It can be the PDU session ID or IP address of the MA PDU session, given that both the UE and the SMF have the PDU session ID and IP address of the MA PDU session.

When deriving a PSK in the SMF or the AMF and the UE, the following parameters are used to form the input S to the KDF:

- FC = TBD

- P0 = ID of the MA PDU Session or IP address of the MA PDU Session

- L0 = Length of P0

- P1 = SUPI

- L1 = Length of P1

The input key KEY could be the KAMF or KSEAF or an intermediate key derived from KAMF or KSEAF.

Editor’s Note: The impact on the SMF for key handling is to be captured in the evaluation clause.

The intermediate key derived from KAMF or KSEAF could be the KSMF, which is derived using the following parameters to form the input S to the KDF:

- FC = TBD

- P0 = SMF instance ID

- L0 = Length of P0

The input key KEY could be the KAMF or KSEAF.

Editor’s Note: The use of KSEAF requires the storage of KSEAF. The impact on the legacy handling of KSEAF is to be captured in the evaluation clause.

### 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 23.501: "System architecture for the 5G System (5GS)".

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