**3GPP TSG-SA3 Meeting #124 S3-253717**

**Wuhan, China, 13 – 17 October 2025 is the revision of S3-253410**

**Source: Huawei, HiSilicon**

**Title: New solution on two layer PSK generation method**

**Document for: Approval**

**Agenda item: 5.2.5**

**Spec: TR 33.778**

**Version: 0.0.0**

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

**Comments**

This contribution proposes a solution on two layer PSK generation method.

The AMF generates a KSMF and sends it to the SMF, and then the SMF generates the KUPF and sends it to the UPF.

The AMF will reuse the existing key generation method in A.13 of TS 33.501.

“

# *A.13 KAMF to KAMF' derivation in mobility*

*Derivation of KAMF' from KAMF during mobility shall use the following input parameters.*

*- FC = 0x72*

*- P0 = DIRECTION*

*- L0 = length of DIRECTION (i.e. 0x00 0x01)*

*- P1 = COUNT,*

*- L1 = length of COUNT (i.e. 0x00 0x04)*

*The input key KEY shall be KAMF.*

*When KAMF' is derived in handover, DIRECTION shall be 0x01 and COUNT shall be the downlink NAS COUNT of the 3GPP access.*

*When KAMF' is derived in idle mode mobility (i.e., mobility registration update), DIRECTION shall be 0x00 and COUNT shall be the uplink NAS COUNT of the 3GPP access used in the Registration Request.*

”

By setting the P0 to another value, the method can be used to generate the KSMF. This method can further be used at SMF, too. By setting the KEY to KSMF, and the P0 to a third value.

By this way, the change to the UE and core network functions is the minimum.

\* \* \* 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] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[z] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

\* \* \* Next Change \* \* \* \*

## 6.Y Solution #Y: two layer PSK generation method

### 6.Y.1 Introduction

This solution proposes a two layer key generation. The AMF will use KAMF generates a Key KSMF and send the KSMF to the selected SMF. The SMF will further generate KUPF using KSMF, and then deliver the key KUPF to the UPF. Meanwhile, the SMF also generates a key ID, and the Key ID is also sent to the UPF together with the KUPF.

### 6.Y.2 Solution details

#### 6.Y.2.1 The procedure for PSK retrieval



Figure 6.Y.2-1 Procedure to get a PSK between UE and UPF for MPQUIC

1. UE sends PDU Session Establishment Request message to the AMF. The message contains the MAP PDU session information defined in TS 23.502[x] and a PSK capability indication. The PSK capability indication is to indicate that the UE supports to generate a PSK for the MPQUIC/TLS between UE and UPF.

2. The AMF selects a SMF that supports MA PDU as described in TS 23.502[x].

3. The AMF sends Nsmf\_PDUSession\_CreateSMContext Request. The message includes the MA PDU session information and the PSK capability indication.

4. The SMF decides MPQUIC may be used based on the decision as defined in TS 23.502[x], and knows the UE supporting to generate a PSK based on the PSK capability indication.

5. The SMF request the KSMF by sending a request message to the AMF. The message includes the SUPI of the UE.

6. The AMF generates the KSMF, and sends the KSMF to the SMF in the response message.

NOTE: this solution will not address the message name in step 5 and step6.

7. The SMF uses the KSMF to generate a KUPF  and a Key ID.

8. the SMF sends a N4 Session Establishment/modification Response to the UPF. In addition to what is defined in TS 23.502[xx], the message further includes the KUPF  and a Key ID.

10 – 12. As defined in TS 23.502[x].

13. The UE generates the KSMF, the KUPF  and the Key ID the same way as AMF and SMF before the UE starts to use MPQUIC.

14. The UE sends a Client Hello message to the UPF, the message contains the Key ID.

15. The UPF uses the Key ID to retrieve the KUPF. The KUPF is used as the PSK for MPQUIC/TLS.

16. The UPF replies a Server Hello message to the UE.

17. The rest of MPQUIC procedure.

Editor’s Note: roaming scenario is FFS.

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

#### 6.Y.2.2 Key hierarchy



Figure 6.Y.2-2 Key hierarchy for KUPF retrieval

Based on the procedure in clause 6.Y.2.1, the AMF generates the KSMF by using the KAMF and deliver it to the SMF, and then the SMF uses the KSMF to generate the KUPF that will be further delivered to the UPF.

#### 6.Y.2.3 KSMF generation method

The KSMF is generated by KAMF reusing the method in A.13 of TS 33.501[y] with the following updated:

- Set the P0 input parameter DIRECTION to the value 0x02.

#### 6.Y.2.4 KUPF generation method

The KUPF is generated by KSMF using the method in A.13 of TS 33.501[y] with the following updated:

- Set the input KEY to KSMF.

- Set the P0 DIRECTION to 0x01.

- Set the COUNT value is set to the value of PDU session ID.

#### 6.Y.2.5 Key ID generation method

The Key ID is generated by KSMF using the method in A.3 of TS 33.535[z] with the following updated:

- Set the input key KAUSF to KSMF.

- Set the P0 = "A-TID" to P0 = "UPF Key ID”.

- Set the L0 = length of "A-TID"; (i.e. 0x00 0x05) to L0 = length of " UPF Key ID "; (i.e. 0x00 0x05).

### 6.Y.3 Evaluation

The solution considers the backward compatible issue to let the SMF knows whether the UE is upgraded to support generating PSK.

In 3GPP system, all PSKs in the key hierarchy are delivered in one hop only. Thus deliver the PSK to the UPF from SMF is not fully comply with the principle. In case that no new interface is introduced directly between AMF and UPF, it is better the AMF generate a middle key for SMF, and then the SMF generates the key for UPF. The less nodes know the PSK, the better.

The key generation method is based on existing method, the solution proposes to reuse the existing key generation as much as possible. If a parameter can be updated to achieve the goal, then no need to introduce a fully new key generation scheme.

A Key ID is used for UPF to find the right PSK.

This solution needs to change SMF to support storage of KSMF and generation of KUPF and a key ID.

Editor’s Note: Further evaluation is FFS.

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