**3GPP TSG-SA3 Meeting #116 *draft\_S3-242572-r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: Nokia, Lenovo**

**Title:** **Solution for authentication, confidentiality, and integrity protection of UE in ATSSS while selecting MPQUIC**

**Document for: Approval, Information, Discussion**

**Agenda Item: 5.15**

# 1 Decision/action requested

***Solution to be approved as part of the TR 33.754***

# 2 References

[1] 3GPP TR 33.754 Study on security aspects for Multi-Access (DualSteer + ATSSS Ph-4)

# 3 Rationale

The contribution proposes a solution for KI#1 and KI#2 of TR 33.754 [1].

# 4 Detailed proposal

\*\*\*\**START of 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".

[2] 3GPP TR 23.700-54 "Study on Multi-Access (DualSteer and ATSSS\_Ph4)".

[3] 3GPP TS 33.501: " Security architecture and procedures for 5G system"

[4] 3GPP TS 23.501: "System architecture for the 5G System (5GS) "

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[y] IETF draft-ietf-quic-multipath-07: "Multipath Extension for QUIC".

\*\*\*\**END of FIRST CHANGE\*\*\**

\*\*\*\**START of SECOND CHANGE\*\*\**

## 6.Y Solution #Y: Authentication, confidentiality, and integrity protection of UE in ATSSS while selecting MPQUIC

### 6.Y.1 Introduction

This solution addresses the security requirements exposed in key issue #1 and key issue #2.

It is assumed that the UE has been registered in 5GC via 3GPP or non-3GPP access and that a Multi-Access PDU session has been established.

The solution relies on the following principles:

- The UE has already been registered and authenticated (primary authentication) in 5GC.

- MPQUIC [y] steering functionality has been selected to provide multipath transport between the UE and the UPF. Therefore TLS 1.3 provides authentication, confidentiality and integrity protection in all configured paths.

- TLS 1.3 Pre-shared Key (PSK) mode, which performs authentication based on symmetric keys, is selected.

- PSK-only is selected as key exchange mode.

- PSKs are generated and derived from the 5GS keys used in the security procedures between UE and 5GS, e.g., KAMF as a root key.

### 6.Y.2 Solution details

Figure 6.Y.2-1 depicts the basic protocol stack in UE and UPF connected via different types of accesses, i.e., 3GPP, Non-3GPP and Non-Integrated Non-3GPP access networks.



Figure 6.Y.2-1: UP protocol stack between UE and UPF with MPQUIC is used as multipath protocol

The security mechanisms for authentication, confidentiality and integrity protection are provided by MPQUIC layer, i.e., TLS 1.3, and are equally applied to all paths, including those transported over non-3GPP types of access.

Figure 6.Y.2-2 illustrate the procedure to establish TLS 1.3 PSK mode in this scenario.



Figure 6.Y.2-2: Procedure to establish TLS 1.3 PSK mode in MPQUIC used in ATSSS

0. Primary authentication between UE and 5GC

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

2a. SMF requests AMF to generate a Pre-Shared Key to be derived from KAMF via a shared random/constant value.

2b. AMF generates the Pre-Shared Key and provides it to the SMF.

2c. UE generates the same Pre-Shared Key.

3. UPF fetches the PSK from SMF.

4. TLS 1.3 PSK mode starts, authentication based on the derived pre-shared key is performed, and traffic between UE and UPF is confidentiality and integrity protected at QUIC layer.

Editor’s note: The details of the pre-shared key derivation procedure are ffs.

### 6.Y.2 Evaluation

The solution works at MPQUIC level, and therefore support mutual authentication via TLS 1.3 between UE and UPF accessing the network via 3GPP and/or non-3GPP access. Additionally, TLS 1.3 ensures confidentiality and integrity protection in the communication between the UE and UPF.

The solution impacts different components of ATSSS architecture as follows:

- UE: the UE generates of a new pre-shared key derived from KAMF via a shared random/constant value, and uses it for TLS authentication.

- AMF: the AMF generates of a new pre-shared key derived from KAMF via a shared random/constant value.

- SMF: the SMF fetches the pre-shared key and provides it to UPF.

- UPF: the UPF receives the pre-shared key and use it for TLS authentication.

\*\*\*\**END of SECOND CHANGE\*\*\**