**3GPP TSG-SA3 Meeting #116 *draft S3-242574-r1***

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

**Source: Ericsson**

**Title: Solution for KI#1 & #2**

**Document for: Approval**

**Agenda Item: 5.15**

# 1 Decision/action requested

***It is proposed to add this solution to the TR in [1]***

# 2 References

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

# 3 Rationale

This document proposes a solution for key issues #1 and #2 of the TR 33.754 [1].

# 4 Detailed proposal

\*\*\*START CHANGES\*\*\*

# 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) "

[X1] RFC 9000; "QUIC: A UDP-Based Multiplexed and Secure Transport"

[X2] RFC 9001: "Using TLS to Secure QUIC"

[X3] draft-ietf-quic-multipath-07 "Multipath Extension for QUIC "

[X4] RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3"

…

\*\*\*NEXT CHANGE\*\*\*

## 6.Y Solution #Y: UE authentication and traffic protection in ATSSS-Lite

### 6.Y.1 Introduction

This solution addresses key issues #1 and #2.

### 6.Y.2 Solution details

#### 6.Y.2.1 Background

There are several potential architectures provided in the TR 23.700-54 [2]. This solution aims at performing an analysis of the architecture proposed in Solution #2.8 of TR 23.700-54 [2] in relation to the security requirements in KI#1 and KI#2.

Solution #2.8 of TR 23.700-54 [2] is based on the architecture displayed in Figure 6.Y.2-1 (copied from [2]), where there is no N3IWF/TNGF used between UE and UPF. There is no N1 connection and hence no NAS connection between UE and 5GC over non-3GPP access.

The solution assumes the use of a Multi access PDU (MA PDU) session using MPQUIC [X3]. Further, the solution assumes that the MA PDU session is established over 3GPP access. After that the UE can get user plane resources over non-3GPP access by adding a QUIC path that will run over non-3GPP access.



Figure 6.Y.2.1-1: Architecture for simplified ATSSS over non-3GPP based on direct MPQUIC connection between UE and UPF as described in Solution #2.8 of 23.700-54.

#### 6.Y.2.2 UE authentication and PDU establishment over 3GPP access

UE authenticates and registers to the 5GC using existing procedures. Once registered, the UE continues to setup a MA PDU session with the selected UPF. The SMF selects a UPF that supports this type of ATSSS. How this is performed is described in the two options of Solution #2.8 of [2] but has no security impact. The UPF also receives an indication for "direct ATSSS via non-3GPP access using MPQUIC".

The UPF allocates MPQUIC proxy information for both the N3 tunnel used via 3GPP access and for the Nx interface (non-3GPP access), i.e. the UPF allocates separate IP addresses and ports of the MPQUIC proxy in UPF for N3 and Nx interfaces (server side IP addresses and ports). The UPF also allocates the IP address for the UE to be used over the 3GPP access but not an address for non-3GPP access. (The UE for its non-3GPP access gets its IP address for the non-3GPP access.)

The information generated by the UPF is transferred to the UE via SMF-AMF. The information is protected over N1 using NAS security.

The UE then establishes a Multipath QUIC connection over the 3GPP access. The UE can also choose to setup multiple QUIC connections, one for each QoS flow, but for the rest of this analysis, we assume only one Multipath QUIC connection to be used with 2 paths, one for 3GPP and one for non-3GPP.

The QUIC connection is secured using a TLS 1.3. During the establishment, the UE authenticates the UPF (server side only authentication). Hence, the UE is not explicitly authenticated by the UPF, only implicitly, since only a UE authenticated by the 5GC can setup a PDU session via SMF. This is not unique for ATSSS, but this is true for all PDU session establishment.

For each QUIC connection the UE obtains the following information from the UPF using inherent QUIC mechanisms:

- At least two Connection IDs for a QUIC connection: A QUIC connection can be associated with multiple Connection IDs. To support multi-path QUIC operation, the QUIC endpoints shall use different Connection IDs on different paths (see [X3]). In this case, a minimum of two separate Connection IDs will be used, one for the 3GPP access and one for the non-3GPP access.

#### 6.Y.2.3 UE authentication over non-3GPP access

Once a MP QUIC connection is established via 3GPP access, the UE can add non-3GPP access user plane resources.

Figure 6.Y.2.3-1 (copied from [2]) shows the procedures for adding a path over non-3GPP access.

1. UE has an established MPQUIC connection with the UPF over 3GPP access. During the setup of the MP QUIC connection, at least 2 Connection IDs were allocated, one used over 3GPP access and the other to be used over non-3GPP access.

2. UE obtains a local IP address from the non-3GPP access.

3. UE initiates the path validation of the new path with the UPF via non-3GPP access as defined in the QUIC specification [X1] and the QUIC multi-path extensions ([X3]). The path validation enables the UPF to verify the IP address of the UE.

The path validation is performed using the same QUIC connection and the same security context as being used for the path over 3GPP access. Hence there is no explicit authentication of the UE over non-3GPP access. From the UPF perspective this is the same UE using the same QUIC connection over an added path. The UPF is not aware of the underlying access type.

4-6. As specified in solution #2.8 of [2]

7. The UE and UPF can start sending data packets via the new path. The data is confidentiality and integrity protected.

Solution #2.8 further specifies that the UPF shall block incoming traffic to the MPQUIC proxy address for non-3GPP access that is not associated to existing QUIC connections. This ensures that only UEs with valid QUIC connections can communicate with the UPF via non-3GPP access.



Figure 6.Y.2.3-1: Addition of non-3GPP access user-plane resources

### 6.Y.3 Evaluation

#### 6.Y.3.1 UE authentication (KI#1)

The UE is authenticated over 3gpp access using existing primary authentication procedures. The authenticated 3gpp access is used for setting up the QUIC (TLS) connection. The same QUIC connection and hence the same security context is used for the non-3gpp access. UPF does not see this as a new access, simply a new path using the same security context.

#### 6.Y.3.2 Confidentiality and integrity protection (KI#2)

Both paths apply confidentiality and integrity protection using credentials established during the setup of the QUIC connection which is using TLS 1.3 [X4].

#### 6.Y.3.3 Privacy considerations (KI#1)

A fresh Connection ID is used for each new path (or when migrating from one path to another) as defined in the QUIC RFC [X1]. The Connection IDs are pre-allocated by the server (UPF) during the QUIC connection establishment. Usage of fresh Connection IDs prevents the linking of different paths to one another.

#### 6.Y.3.4 System impact

Impacted entities are:

- UE

- AMF/SMF (depending on option 1 or option 2 of Solution #2.8 of TR 23.700-54 [2])

- UPF

\*\*\*END OF CHANGES\*\*\*