**3GPP TSG-SA3 Meeting #116  *S3-242058-r1***

**Jeju Island, S.Korea, May 20 – May 24, 2024**

**Source: Intel**

**Title: Secure Authentication and Connectivity for UE in ATSSS over NIN3A**

**Document for: Approval**

**Agenda Item: 5.15**

# 1 Decision/action requested

***Approve the pCR to TR 33.754***

# 2 References

# 3 Rationale

This contribution proposes a new solution to Key issues 1 and 2

# 4 Detailed proposal

SA3 is requested to approve the following pCR.

\*\*\*\*\*START CHANGE\*\*\*\*\*

6.Y Solution #Y: Secure Authentication and Connectivity for UE in ATSSS over NIN3A

6.Y.1 Introduction

This solution addresses the key issue of securely authenticating the UE in ATSSS over Non-Integrated Non-3GPP Access (NIN3A), as outlined in section 5.1(key issues 1 and 2).

6.Y.2 Solution details

The proposed solution introduces a secure mechanism for UE authentication and connectivity in ATSSS over NIN3A, leveraging the MP-QUIC protocol. Figure 3 depicts the call flow describing the provision of security material to the UE.



The solution involves the following steps:

1. The UE sends a PDU Session Establishment Request message and includes within the PDU session establishment Request message the ATSSS capabilities it supports, as per existing specifications.

2. The AMF selects an SMF which is capable of the specific ATSSS feature indicated to be supported by the UE and sends a Nsmf\_PDUSession\_Create Request message with the PDU Session Establishment Request message, as per existing specifications.

3. The SMF interacts with UDM as per existing specifications.

4. The SMF replies to AMF with an Nsmf\_PDUSession\_Create Response, as per existing specifications.

5. The SMF initiates a SM Policy Session Establishment and indicates the MA PDU Session capabilities, as per existing specification.

6. The SMF selects a UPF supporting ATSSS using MPQUIC.

 The SMF sends a N4 Session Establishment Request message to the UPF and includes the required ATSSS features that should be activated in the UPF. The SMF also provides N4 rules, e.g. MAR, to the UPF.

The UPF allocates MPQUIC proxy information and a UE "MPQUIC link-specific multipath" address/prefix for 3GPP and non-3GPP access, as per existing specifications.

In case of certificate-based authentication between UE and UPF, or receiving a PSK key based on existing security association between UE and CN , following PSK handling and in steps 7-8 is not required.

The UPF generates a Pre-Shared Key (PSK), to be used as security material for mutual authentication while establishing the MPQUIC connection (step 10).This is similar to issuing a ticket for session resumption in TLS 1.3, where the server provides a PSK to the client at the end of a handshake. Alongside the PSK, the UPF generates a PSK ID. This ID serves as a reference that can either uniquely identify the PSK within the UPF's database or securely encapsulate session state information. The PSK ID is designed to prevent tampering and ensure secure retrieval of the PSK. The UPF securely stores the PSK and its corresponding PSK ID in a session context database

The UPF replies with a N4 Session Establishment Response message and provides the UE "MPQUIC link-specific multipath" addresses/prefixes for 3GPP and non-3GPP access, the MPQUIC proxy information and the PSK to the SMF.

7-8. The SMF sends the PDU Session Establishment Accept to the UE and includes the following information:

- MPQUIC Proxy information

- Link-Specific Multipath IP address for 3GPP access and non-3G¨P access, as defined in TS 23.501, clause 5.32. The MPQUIC functionality in the UE and the MPQUIC Proxy functionality in the UPF shall use the "MPQUIC link-specific multipath" addresses/prefixes for proxying traffic flows over 3GPP access, as defined in TS 23.501, clause 5.32.6.

- Pre-Shared Key (PSK)

Editor’s Note: potential security issues coming from transmitting the pre-shared keys to the UE are ffs

 The SMF may also include ATSSS rules.

9. The rest of the MA PDU Session procedure is executed, as described in TS 23.502.

10. After the MA PDU Session establishment, the UE determines to establish at least as many multipath QUIC connections as the number of QoS flows of the MA PDU Session, i.e. one multipath QUIC connection per QoS flow, as described in TS 23.501 and TS 23.502. These multipath QUIC connection are established via the access on which the MA PDU Session was established, allowing the UPF to associate the QUIC connection with the PDU Session / N3 tunnel.

 During the establishment of a MP-QUIC connection, the MPQUIC client in the UE and the MPQUIC Proxy in the UPF mutually authenticate each other using TLS-PSK ciphersuite based on the PSK that was provided to the UE in the PDU Session Establishment Accept message. The UE initiates the MPQUIC connection setup by sending initial QUIC packets to the UPF. As part of these packets, the UE includes the pre\_shared\_key extension, offering the PSK ID obtained during the PDU Session Establishment. For PSKs used in session resumption, the UE populates the obfuscated\_ticket\_age field within the identity offered in the pre\_shared\_key extension. This field is set to zero for PSKs not used for session resumption. If PSK authentication is accepted by the UPF (the server), it indicates the selected identity from the pre\_shared\_key extension. Both parties then use the selected PSK to generate connection key material and complete the handshake, leveraging the psk\_dhe\_ke option for forward secrecy.

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 IETF draft-ietf-quic-multipath).

- Token for Address Validation: The UE shall present a token in the initial QUIC handshake to prove its IP address to the UPF, mitigating against potential spoofing and amplification attacks. This token is used as part of QUIC's path validation mechanism.

6.Y.3 Evaluation

The proposed solution fulfills the potential security requirements for UE authentication in ATSSS over NIN3A by introducing a secure and efficient mechanism for UE authentication and connectivity. MP-QUIC with PSK authentication ensures the UE's identity is securely verified and authenticated before establishing a direct connection to the UPF. Additionally, the solution protects the UE's identity during the connectivity process, addressing the primary concerns of authentication privacy and identity protection.

The solution leverages the Multi-Path QUIC (MP-QUIC) protocol, which inherently supports confidentiality and integrity protection by using TLS 1.3 for encryption. The Pre-Shared Key (PSK) mechanism introduced for mutual authentication between the UE and the UPF also plays a crucial role in ensuring communication security.

Editor’s Note: the steps running through 3GPP access and non-3GPP access needs to be clarified.

Editor’s Note: System Impact is FFS.

\*\*\*\*\*END CHANGE\*\*\*\*\*