|  |
| --- |
| 3GPP TR 33.754 V0.3.0 (2024-08) |
| *Technical* *Report* |
| **3rd Generation Partnership Project;****Technical Specification Group Services and System Aspects;****Study on security aspects for Multi-Access(DualSteer + ATSSS Ph-4);****(Release** **19)** |
|   |
| *A logo with a green logo  Description automatically generated* | 3GPP-logo_web |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

4 Security assumptions 9

5 Key issues 9

5.1 Key Issue #1: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access 9

5.1.1 Key issue details 9

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access. 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

6 Solutions 11

6.0 Mapping of solutions to key issues 11

6.1 Solution #1: Using 3GPP security context to derive authentication pre-shared key for NIN3A 11

6.1.1 Introduction 11

6.1.2 Solution details 11

6.1.3 Evaluation 12

6.2 Solution #2: AUSF based authentication mechanism for UE and UPF 12

6.2.1 Introduction 12

6.2.2 Solution details 13

6.2.1 Delivery of UPF information 13

6.2.2 Authentication based on AUSF 13

6.2.3 Evaluation 14

6.3 Solution #3: Authentication, confidentiality, and integrity protection of UE in ATSSS while selecting MPQUIC 14

6.3.1 Introduction 14

6.3.2 Solution details 15

6.3.2 Evaluation 16

6.4 Solution #4: Secure Authentication and Connectivity for UE in ATSSS over NIN3A 16

6.4.1 Introduction 16

6.4.2 Solution details 16

6.4.3 Evaluation 19

6.5 Solution #5: UE authentication and traffic protection in ATSSS-Lite 19

6.5.1 Introduction 19

6.5.2 Solution details 19

6.5.2.1 Background 19

6.5.2.2 UE authentication and PDU establishment over 3GPP access 20

6.5.2.3 UE authentication over non-3GPP access 21

6.5.2.4 UPF IP address exposure 22

6.5.3 Evaluation 22

6.5.3.1 UE authentication (KI#1) 22

6.5.3.2 Confidentiality and integrity protection (KI#2) 23

6.5.3.3 Privacy considerations (KI#1) 23

6.5.3.4 System impact 23

6.6 Solution #6: Using IPsec to authenticate UE and UPF for non-3GPP access 23

6.6.1 Introduction 23

6.6.2 Solution details 23

6.6.3 Evaluation 25

6.7 Solution #7: Omitting IPsec for MPQUIC traffic over non-3GPP access 25

6.7.1 Introduction 25

6.7.2 Solution details 26

6.7.3 Evaluation 27

6.8 Solution #8: User plane data protection mechanism between UE and UPF 27

6.8.1 Introduction 27

6.8.2 Solution details 28

6.8.3 Evaluation 28

7 Conclusions 28

7.1 Key Issue #1: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access 28

7.2 Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access. 28

Annex <X> (informative): Change history 29

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document aims to address the security aspects of Multi-Access, focusing on DualSteer devices and ATSSS Phase 4 (ATSSS Ph-4) enhancements, as identified in the FS\_MASSS study in TR 23.700-54 [2].

The scope of this study includes the following key areas:

- Examine the security implications of a simplified architecture over non-3GPP access, where non-3GPP access does not rely on the current TNGF/N3IWF architecture. This involves assessing:

- Whether to keep NAS security context on non-3GPP access.

- Whether to keep IPsec on the user plane and/or control plane of non-3GPP access.

- Whether new security mechanisms are to be considered in UE procedures, particularly regarding registration and connectivity to the 5G system in the context of ATSSS between 3GPP and non-3GPP access without 5G NAS.

The study will leverage insights from the requirements and architectural considerations outlined in the FS\_MASSS study in TR 23.700-54 [2].

# 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) "

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

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

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

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

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

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

[X1] [draft-ietf-quic-load-balancers-19 - QUIC-LB: Generating Routable QUIC Connection IDs](https://datatracker.ietf.org/doc/draft-ietf-quic-load-balancers/)

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Non-Integrated Non-3GPP Access:** as defined in TR 23.700-54[2].

**example:** text used to clarify abstract rules by applying them literally.

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

NIN3A Non-Integrated Non-3GPP Access
ATSSS Access Traffic Steering, Switching, and Splitting
MP-QUIC Multipath QUIC

# 4 Security assumptions

Void

# 5 Key issues

## 5.1 Key Issue #1: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access

### 5.1.1 Key issue details

As specified in TS 33.501 [3], authentication of UE for non-3GPP access is done by the successfully running the primary authentication. However, TR 23.700-54 [2] introduces the concept of Non-Integrated Non-3GPP Access (NIN3A), a type of non-3GPP access network that provides direct IP connectivity between the UE and the UPF without any intermediate NF such as Non-3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNFG). Here, UE does not register to the 5GC over this Non-Integrated Non-3GPP Access. However, the UE is still able to access 5G resources, i.e. UPF, SMF. NIN3A leverages direct connections between UE and UPF to streamline connectivity.

This Key Issue focuses on the security challenges associated with direct connectivity, particularly in the absence of N3IWF/TNGF. The primary concerns include:

- Authentication: Ensuring the UE's identity is securely verified and authenticated before establishing a direct connection to the UPF.

- Privacy and Identity Protection: Protecting the UE's identifier during the connectivity process.

### 5.1.2 Security threats

Non-Integrated Non-3GPP Access (NIN3A) exposes a new IP communication endpoint in the 5G Core (UPF) to be reachable directly by the UE. The absence of authentication between the UE and UPF introduces significant security risks and threats, potentially compromising the UPF network element and the entire 5G Core. Here are some of those threats:

- Unauthorized Access: The lack of authentication would allow unauthorized UEs to gain access and connect directly to the UPF, compromising the network resources and potentially launching further attacks.

- Impersonation: Attackers can spoof the identity of legitimate UEs or masquerade as trusted entities to gain access to the network.

- Denial of Service (DoS) Attacks: Attackers can exploit the lack of authentication to launch DoS attacks against the UPF, overwhelming network resources and disrupting legitimate services.

### 5.1.3 Potential security requirements

The 5G System should support the means to authenticate a UE accessing the network via Non-Integrated Non-3GPP Access (NIN3A).

The authentication mechanism should not compromise the privacy of the UE.

## 5.2 Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access.

### 5.2.1 Key issue details

TR 23.700-54 [2] introduces the concept of non-Integrated non-3GPP Access (NIN3A), a type of non-3GPP access network that provides direct IP connectivity between the UE and the UPF without any intermediate NF such as Non-3GPP Interworking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNFG). This access type should not compromise the security of the 5G network.

This key issue focuses on safeguarding the confidentiality and integrity of data exchanged between the UE and the 5G Core Network under NIN3A connectivity, within the ATSSS framework. It emphasizes the need for comprehensive security measures that encompass both the associated proxy functionalities, such as MPQUIC and MPTCP, as specified for ATSSS in TS 23.501 (clause 5.32) [4], and beyond.

### 5.2.2 Security threats

If the communication between UE and 5G Core Network via NIN3A is not confidentiality and integrity protected, an attacker could intercept and manipulate the traffic between both endpoints, leading to data theft, tampering or service disruption. These vulnerabilities could undermine the trust and reliability of the 5G network, especially in scenarios that leverage NIN3A for enhanced connectivity.

### 5.2.3 Potential security requirements

The new simplified ATSSS architecture over non-3GPP access should provide the mechanisms to protect the traffic between the UE accessing the network via Non-Integrated Non-3GPP Access (NIN3A) and the 5G Core Network.

##

# 6 Solutions

## 6.0 Mapping of solutions to key issues

###

|  |  |  |
| --- | --- | --- |
| **Solutions** | **KI#1** | **KI#2** |
| **#1** | X |  |
| **#2** | X |  |
| **#3** | X | X |
| **#4** | X | X |
| **#5** | X | X |
| **#6** | X |  |
| **#7** | X | X |
| **#8** |  | X |

**Table 6.0-1: Mapping of solutions to key issues**

## 6.1 Solution #1: Using 3GPP security context to derive authentication pre-shared key for NIN3A

### 6.1.1 Introduction

This solution addresses key issue #1.

This solution gives the key architecture for ATSSS-Lite scenario and lists some options about how to derive and obtain the authentication key used for non-3GPP access between UE and UPF.

### 6.1.2 Solution details

In the simplified ATSSS architecture, there is an assumption that UE will establishe connection with network and establish PDU session using 3GPP access. Considering UE and network already generated shared security context during the registration procedure via 3GPP access. A sub-level shared key can be generated, and be used as a pre-shared key for IKEv2 procedure.

The key hierarchy defined in TS 33.501[3] for this scenario can be extended as follows:



**Figure 6.1.2.1 Key hierarchy generation for ATSSS-lite scenario**

A new key KUPF is derived from KAMF as depicted in Figure 6.1.2.1. AMF derives the KUPF from KAMF during the PDU session establishment procedure over 3GPP access as showing in clause 6.1.2 of S3-241982.

When deriving a KUPF from KAMF, the following parameters shall be used to form the input S to the KDF:

- FC = 0xXX,

- P0 = PDU session ID,

- L0 = length of PDU session ID,

- P1 = Uplink NAS COUNT,

- L0 = length of Uplink NAS COUNT.

The input key KEY shall be KAMF.

Regarding with when SMF gets the KUPF in the case the SMF needs to transfer the KUPF, there are several options:

Option 1: AMF sends KUPF to SMF in the CreateSMContext Request message, SMF selects the UPF and sends the key KUPF to UPF.

Option 2: SMF requests the key from AMF and based on the reply, the SMF further sends it to UPF during the PDU session establishment procedure.

Regarding with when UPF gets the KUPF, there are several options as well:

Option 1: UPF requests the key from SMF based on the request from the UE via NIN3A.

Option 2: SMF sends the key to the UPF during the PDU session establishment procedure.

Option 3: SMF requests the key from AMF and AMF sends the key to UPF during the PDU session establishment procedure.

### 6.1.3 Evaluation

This solution addresses key issue #1 and proposes to reuse the current 3GPP security context to generate a sub-level shared key, which can be used as a pre-shared key for the NIN3A authentication procedure.

The UE and AMF have to derive KUPF based on KAMF.

UPF has to obtain KUPF before the non-3GPP access procedure, different options may have different impacts, for example, since there is no direct interface between UPF and AMF, the option where the AMF directly sends KUPF to UPF has a bigger 5G system impact and requires a new interface. Therefore, it is better to select option 1 or option 2, in which cases the impact is limited and requires only the provisioning of new parameters over existing interfaces. SMF needs to be able to handle plaintext keys in a secure way.

## 6.2 Solution #2: AUSF based authentication mechanism for UE and UPF

### 6.2.1 Introduction

This solution addresses KI#1.

The UE and UPF realize mutual authentication based on the shared key, which is derived based on KAUSF.

### 6.2.2 Solution details

#### 6.2.1 Delivery of UPF information



**Figure 6.2.2-1 Delivery of UPF information**

Step 1. The UPF sends UPF information (e.g., FQDN of the UPF) to the SMF.

Step 2. The SMF includes the UPF information in the PDU Session Establishment Accept message. The SMF sends UPF information to the AMF via the accept message.

Step 3. The AMF sends UPF information to the UE via the PDU Session Establishment Accept message.

#### 6.2.2 Authentication based on AUSF

 **Figure 6.2.2-1 Authentication based on AUSF.**

1. The UE sets the SUCI as the PSK identity in the ClientHello message.

NOTE: The usage of SUCI as the PSK identity is not studied.

1. The UPF sends the SUCI to the UDM/ARPF/SIDF to get the SUPI.

The UPF checks the availability of PDU session based on the UE identifier. If no accepted available PDU session is associated with the UE identifier, the UPF rejects the UE request.

If the accepted PDU session information is found available, the UPF sends the AUSF the SUPI and its FQDN to the AUSF.

NOTE: The discovery of AUSF has not been studied.

The AUSF sends back the KUPF and the SUPI to the UPF.

When deriving a KUPF from KAUSF, the following parameters shall be used to form the input S to the KDF:

- P0 =UE identifier (i.e. SUPI);

- L0 = length of UE identifier

- P1 =UPF identifier;

- L1 = length of UPF identifier (i.e., FQDN of UPF)

The input key KEY shall be KAUSF.

NOTE: The derivation of K­UPF is not studied.

1. The UPF sends the SUCI to the UE. The SUCI serves as the PSK identity in the ServerHello message.
2. The UE can also derive KUPF in a similar way. The UE and the UPF can do the mutual authentication based on the shared KUPF.

### 6.2.3 Evaluation

Void

## 6.3 Solution #3: Authentication, confidentiality, and integrity protection of UE in ATSSS while selecting MPQUIC

### 6.3.1 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 [5] 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.

### 6.3.2 Solution details

Figure 6.3.2-1 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 6.3.2-1: 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 6.3.2-2 illustrate the procedure to establish TLS 1.3 PSK mode in this scenario.



**Figure 6.3.2-2: 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.

NOTE: The details of the pre-shared key derivation procedure are not studied.

NOTE: The steps running through 3GPP access and non-3GPP access are not studied.

### 6.3.2 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.

## 6.4 Solution #4: Secure Authentication and Connectivity for UE in ATSSS over NIN3A

### 6.4.1 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).

### 6.4.2 Solution details

The proposed solution introduces a secure mechanism for UE authentication and connectivity in ATSSS over NIN3A, leveraging the MP-QUIC protocol. Figure 6.4.2-1 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)

NOTE: Potential security issues from transmitting the pre-shared keys to the UE have not been studied.

 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.

### 6.4.3 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.

NOTE: The steps running through 3GPP access and non-3GPP access need to be studied.

NOTE: System impact needs to be studied.

## 6.5 Solution #5: UE authentication and traffic protection in ATSSS-Lite

### 6.5.1 Introduction

This solution addresses key issues #1 and #2.

### 6.5.2 Solution details

#### 6.5.2.1 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 6.5.2-1 (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 [8]. 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 6.5.2.1-1: 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.

#### 6.5.2.2 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 from 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, and this is not needed either, 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.

Note that it is not necessary for the client (UE) to authenticate the server (UPF) either in the context of ATSSS, for the same reason as above. TLS however mandates the server to be authenticated, for example by sending its certificate to the client, but it is it is not mandated for the client to verify the certificate using a root certificate. It could for example be a self-signed certificate.

Hence, the UPF needs to be configured with a server certificate and the UE can optionally be configured with the means to verify that certificate.

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 [8]). 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.

#### 6.5.2.3 UE authentication over non-3GPP access

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

Figure 6.5.2.3-1 (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 [6] and the QUIC multi-path extensions ([8]). 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. The credentials are the same as for the first path since both belong to the same QUIC connection.

Solution #2.8 of TR 23.700-54 [2] 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 6.5.2.3-1: Addition of non-3GPP access user-plane resources

#### 6.5.2.4 UPF IP address exposure

In this solution, the UPF is accessed directly by the UE, not via any GW such as the Rel-18 architecture where a N3IWF is placed between UE and UPF. This means that UPF exposes an interface to the Internet. This interface must be able to receive packets from any internet host, which can be seen as a vulnerability.

The MPQUIC server in the UPF needs to do some sanity checks of its own:

* Connection ID: As already mentioned in 6.5.2.3, the UPF needs to block incoming traffic to the MPQUIC proxy address that is not associated to existing QUIC connections (based on Connection ID).

To further protect the UPF, additional security measures can be applied. However, such security measures are33.7 out of scope of 3gpp.

### 6.5.3 Evaluation

#### 6.5.3.1 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 MPQUIC (TLS) connection. The MPQUIC connection is established using server-side authentication based on certificates. Hence, the UE is not explicitly authenticated by the UPF, and this is not needed either, since only a UE authenticated by the 5GC can setup a PDU session via SMF and the MPQUIC connection is established over the PDU session. This is not unique for ATSSS, but this is true for all PDU session establishments

The same MPQUIC 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.

#### 6.5.3.2 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 [9].

#### 6.5.3.3 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 [6]. 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.

#### 6.5.3.4 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

## 6.6 Solution #6: Using IPsec to authenticate UE and UPF for non-3GPP access

### 6.6.1 Introduction

This solution addresses key issue #1.

 The authentication of UE during the IKEv2 procedure can be optimized by using the 3GPP security context for the same UE.

### 6.6.2 Solution details

In simplified ATSSS architecture, there is an assumption that UE will establish connection with network and establish PDU session using 3GPP access. In that case, before UE connects to UPF through NIN3A, UE and network already shared security context for 3GPP access. So, the authentication method of IKEv2 protocol for non-3GPP access can utilise pre-shared key between UE and UPF instead of EAP-5G method. The specific procedure is as follows:

 

**Figure 6.6.2.1 ATSSS-lite authentication procedure over NIN3A**

1. 3GPP registration procedure is executed between UE and network through 3GPP access.

2. UE sends PDU session request to AMF through 3GPP access which carries an ATSSS-Lite indication.

3-4. AMF selects ATSSS-lite enabled SMF and forwards PDU session request to SMF.

5. SMF selects ATSSS-lite enabled UPF and obtains an authentication key KUPF for the direct connection between the UE and the UPF. Then the SMF initiates the N4 Session Establishment procedure with the selected UPF and sends the KUPF to UPF.

6. The UPF allocates the IP address for the IPSec functionality of the UPF and responds to the SMF the N4 Session Establishment Accept message including the UPF IP address which is to be used for establishment of the IPSec tunnel with the UE.

7. UPF IP address is sent to UE along with the PDU session accept message.

8. UE derives the key KUPF used for authentication between UE and UPF.

9. Data Link Layer L2 is connected.

10.The UE starts the IPSec Tunnel Establishment procedure to the UPF indicated by the UPF IP address received in PDU Session Establishment Accept message via 3GPP access, and exchanges the first pair of messages known as IKE\_SA\_INIT.

11.UE sends the IKE\_AUTH\_request to the UPF with the Authentication Method “Shared Key Message Integrity Code” (i.e. the value of authentication method is “2”), and the MAC value (MAC1) carried in the AUTH payload is constructed using the derived key KUPF in step 8.

12.The UPF will check the validity of MAC value carried in AUTH payload using the KUPF as described in step 5. If the verification is passed, UPF constructs AUTH payload as in step 11 (with authentication method is “2”, and MAC2 constructed from KUPF) and sends it to UE.

UE checks the validity of AUTH payload using the KUPF and if the verification passed the authentication of UPF to UE is also passed.

13. UE and UPF run the CREAT\_CHILD\_SA procedure and establish the IPsec security tunnel.

### 6.6.3 Evaluation

This solution addresses key issue #1 and proposes to use IKEv2 protocol to do the authentication during the non-3GPP access procedure for NIN3A scenario.

It requires that the UE and UPF supports the functionality of IKEv2 using a pre-shared key-based authentication method.

UE and UPF have to obtain a pre-shared key before the non-3GPP procedure starts, the key can be derived according to the mechanism defined in solution #1.

## 6.7 Solution #7: Omitting IPsec for MPQUIC traffic over non-3GPP access

### 6.7.1 Introduction

This solution addresses Key Issue #1: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access and Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access.

The solution is applicable for trusted or untrusted non-3GPP access, where the AMF provides an UPF address to the UE and an UPF key to the UPF so that UE and UPF can establish the TLS connection for MPQUIC with the UPF key directly and outside the IPsec connection between UE and Non-3GPP access network.

### 6.7.2 Solution details



**Figure 6.7.2-1 Omitting IPsec for QUIC traffic over non-3GPP access**

1. The following steps are according to steps 1-5 of clause “7.2.1 Authentication for Untrusted non-3GPP Access” or clause “7A.2.1 Authentication for trusted non-3GPP access” of 3GPP TS 33.501. The UE connects to a non-3GPP access network and sends a NAS Registration Request message (the NAS message is sent via different protocols depending on the non-3GPP access type) containing UE security capabilities and the SUCI and an indication that the UE supports MPQUIC/non-Integrated non-3GPP Access (NIN3A).

2. The Non-3GPP Access shall select an AMF and forwards the Registration Request with the indication that the UE supports MPQUIC/ NIN3A to the AMF.

3. The AMF initiates the authentication procedure between AUSF and the UE following the normal procedures.

4. The AMF performs the NAS SMC operation following the normal procedures.

5. The AMF upon reception of the NAS SMC Complete from the UE or upon success of integrity protection verification, initiates the NGAP procedure to set up the AN context. AMF shall compute the Non-3GPP Access key, KTNGF or KN3IWF, using the uplink NAS COUNT associated with NAS connection identifier "0x02" for the establishment of the IPsec SA between the UE and the N3IWF and shall include it in the N2 Initial Context Setup Request sent to the Non-3GPP Access.

6. The UE and the AMF shall derive the UPF key similar to the Non-3GPP Access key, i.e. NAS connection identifier "0x02" and Uplink NAS COUNT shall be set to 0 to avoid that the KUPF is the same key as the KTNGF or KN3IWF. The AMF selects the UPF.

7. The AMF sends a UPF Context Setup message to the UPF, containing the UE Identity (Subscription Permanent Identifier (SUPI), Generic Public Subscription Identifier (GPSI), etc.) and the UPF key KUPF. The message may be sent via the SMF.

8. The UPF stores the key KUPF and the UE ID and acknowledges the message towards the AMF. The message may be sent via the SMF.

9. The IPsec SA is established between the UE and Non-3GPP Access by using the Non-3GPP Access key KTNGF or KN3IWF .

10. The AMF sends the NAS Registration Accept message including the UPF address to the Non-3GPP Access.

11. The Non-3GPP Access shall forward the NAS Registration Accept message including the UPF address to the UE over the established IPsec SA. All further NAS messages between the UE and the N3IWF shall be sent over the established IPsec SA.

12. The UE sets up the MPQUIC session towards the UPF outside the IPSec SAs between UE and the N3IWF. The UE and the UPF use the KUPF for mutual authentication and the TLS session setup, i.e. as input for the algorithms for confidentiality and integrity protection.

NOTE: whether the NAS message is sent and whether the Registration Request message is used over non-3GPP access fulfills the architecture requirement is not studied.

NOTE: The new interface between AMF and UPF has not been studied.

NOTE: The method of generating Kupf has not been studied.

### 6.7.3 Evaluation

The solution is independent of the untrustred o trusted non-3GPP access typ.

NOTE: The solution is limited to non-3GPP access,

NOTE: further evaluation is not studied.

NOTE: System impact is not studied.

## 6.8 Solution #8: User plane data protection mechanism between UE and UPF

### 6.8.1 Introduction

This solution addresses KI#2.

TLS embedded in MPQUIC [10] is used to protect the user plane data between UE and the UPF.

### 6.8.2 Solution details

When MPQUIC is used, TLS embedded in MPQUIC [X] is used to provide integrity protection, replay protection and confidentiality protection for the user plane data protection between the UE and the UPF.

### 6.8.3 Evaluation

Void

# 7 Conclusions

## 7.1 Key Issue #1: Authentication of UE in ATSSS over Non-Integrated Non-3GPP Access

No solution is needed for normative work in this release.

## 7.2 Key Issue #2: Confidentiality and integrity protection of the communication between UE and 5GCore in Non-Integrated Non-3GPP Access.

No solution is needed for normative work in this release.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115Adhoc-e | S3-241591 |  |  |  | TR Skeleton | 0.0.0 |
| 2024-04 | SA3#115Adhoc-e | S3-241608 |  |  |  | Included changes from S3-241590, S3-241577, S3-241366, | 0.1.0 |
| 2024-05 | SA3#116 | S3-242605 |  |  |  | Included changes from S3-242050, S3-242568, S3-242569, S3-242570,S3-242571,S3-242572, S3-242573, S3-242574, S3-242575, S3-242654, S3-242655 | 0.2.0 |
| 2024-08 | SA3#117 | S3-243599 |  |  |  | Included changes from S3-243601, S3-243602, S3-242957, S3-243071, S3-243600,S3-243068, S3-243598 | 0.3.0 |