|  |  |
| --- | --- |
| 3GPP TR 23.700-54 V0.2.0 (2024-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Multi-Access (DualSteer and ATSSS\_Ph4)  (Release 19) | |
|  | |
|  |  |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms and abbreviations 7

3.1 Terms 7

3.2 Abbreviations 7

4 Architectural Assumptions and Requirements 7

4.1 Architectural Assumptions 7

4.1.1 Architectural Assumptions for DualSteer 7

4.1.2 Architectural Assumptions for ATSSS\_Ph4 7

4.2 Architectural Requirements 8

4.2.1 Architectural Requirements for DualSteer 8

4.2.2 Architectural Requirements for ATSSS\_Ph4 8

5 Key Issues 8

5.1 Key Issues for DualSteer 8

5.1.1 Key Issue #1.1: Subscription aspects to support DualSteer 8

5.1.2 Key Issue #1.2: Registration and mobility management for DualSteer 8

5.1.3 Key Issue #1.3: Session management aspects for DualSteer 9

5.1.4 Key Issue #1.4: Policy enhancements for DualSteer 9

5.2 Key Issues for ATSSS\_Ph4 9

5.2.1 Key Issue #2.1: MPQUIC steering functionality to steer, switch and split non-UDP traffic 9

5.2.2 Key Issue #2.2: Simplified ATSSS architecture over non-3GPP access 10

6 Solutions 10

6.0 Mapping of Solutions to Key Issues 10

6.1 Solutions for DualSteer 11

6.1.X Solution #X: <Solution Title> 11

6.2 Solutions for ATSSS\_Ph4 11

6.2.1 Solution #2.1: Policy Control for the MPQUIC Steering Functionality for non-UDP Traffic 11

6.2.2 Solution #2.2: IPsec establishment using null encryption with ePDG co-located in the UPF 14

6.2.3 Solution #2.3: MPQUIC Steering Functionality extended with additional CONNECT methods 16

6.2.4 Solution #2.4: MPQUIC steering functionality using IP proxying over HTTP 20

6.2.5 Solution #2.5: MPQUIC steering functionality using Ethernet proxying over HTTP 28

6.2.6 Solution #2.6: for KI#2.2 36

6.2.7 Solution #2.7: Architecture for ATSSS-Lite 40

6.2.8 Solution #2.8: Simplified ATSSS over non-3GPP based on direct MPQUIC connection between UE and UPF 46

7 Overall Evaluation 53

7.1 Overall Evaluation for DualSteer 53

7.2 Overall Evaluation for ATSSS\_Ph4 53

8 Conclusions 53

8.1 Conclusions for DualSteer 53

8.2 Conclusions for ATSSS\_Ph4 54

# 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 scope of this Technical Report is to:

- study and identify potential architecture and system level enhancements for the 5G system to support the operation of the DualSteer Device that is capable of traffic steering and switching of user data for different services across two 3GPP access networks. The study addresses the service requirements documented in TS 22.261 [2] and focuses on various aspects of architecture and functional enhancements including:

- impacts on subscription;

- impacts on registration procedure; and

- impacts on session management procedure and policies.

- study how the MPQUIC steering functionality defined in Rel-18 ATSSS can be extended to be able to steer, switch, and split non-UDP traffic (TCP, IP, Ethernet traffic); and

- study whether and how an alternative architecture and system level enhancements for ATSSS that does not require the existing non-3GPP interworking/gateway function, i.e., N3IWF, TNGF.

# 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 TS 22.261: "Service requirements for the 5G system".

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

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[5] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[6] IETF RFC 9298: "Proxying UDP in HTTP".

[7] IETF RFC 9484: "Proxying IP in HTTP".

[8] IETF draft-ietf-masque-connect-ethernet: "Proxying Ethernet in HTTP".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[9] IETF RFC 9114: "Hypertext Transfer Protocol Version 3 (HTTP/3)".

[10] IETF draft-ietf-httpbis-connect-tcp: "Template-Driven HTTP CONNECT Proxying for TCP".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[11] IETF RFC 9297: "HTTP Datagrams and the Capsule Protocol".

[12] IETF RFC 9000: "QUIC – A UDP based Multiplexed and Secured Protocol".

[13] IETF RFC 9001: "Using TLS to Secure QUIC".

[14] IETF RFC 9002: "QUIC Loss Detection and Congestion Control".

[15] IETF RFC 9221: "An Unreliable Datagram Extension to QUIC".

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

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[17] 3GPP TR 23.700-53: "Study on access traffic steering, switching and splitting support in the 5G system architecture; Phase 3".

[18] IETF RFC 9369: "QUIC Version 2".

[19] IETF RFC 9220: "Bootstrapping WebSockets with HTTP/3".

[20] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

**Non-Integrated Non-3GPP Access:** 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 (TNGF). When a UE is connected using Non-Integrated Non-3GPP Access, the UE data flows can be routed via this access to operator services.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

<ABBREVIATION> <Expansion>

NIN3A Non-Integrated Non-3GPP Access

# 4 Architectural Assumptions and Requirements

## 4.1 Architectural Assumptions

Editor's note: This clause will document any architectural assumptions for the study.

### 4.1.1 Architectural Assumptions for DualSteer

Editor's note: This clause will document any DualSteer architectural assumptions for the study.

### 4.1.2 Architectural Assumptions for ATSSS\_Ph4

The following general assumptions apply:

- The Rel-18 ATSSS as specified in TS 23.501 [3], TS 23.502 [4], and TS 23.503 [5] are regarded as the baseline for this study.

The following assumptions apply to alternative architecture and system level enhancements for ATSSS that do not require the existing non-3GPP interworking/gateway function:

- Current Non-3GPP InterWorking Function (N3IWF) and Trusted Non-3GPP Gateway Function (TNGF) are not used to simplify the operation over non-3GPP access.

- Any alternative architecture and system level enhancements would also be applicable for a UE behind an RG.

The following assumptions apply to MPQUIC for non-UDP traffic:

- Any new steering functionality shall be based on the multipath extensions of the QUIC protocols as defined in IETF.

- All ATSSS steering functionalities (existing and new) shall reside in the UE and in an UPF. Steering functionalities outside either of the UE or the UPF are not considered.

- Any new ATSSS capabilities specified for UE would be applicable for ATSSS-capable 5G-RGs, if endorsed by BFF and/or CableLabs; FN-RG are not in the scope of the study.

## 4.2 Architectural Requirements

Editor's note: This clause will document any architectural requirements for the study.

### 4.2.1 Architectural Requirements for DualSteer

Editor's note: This clause will document any DualSteer architectural requirements for the study.

### 4.2.2 Architectural Requirements for ATSSS\_Ph4

- New ATSSS capabilities shall either be able to co-exist with the existing ATSSS capabilities or any dependencies between new and existing capabilities shall be explicitly defined.

- The benefit and drawback of new solutions compared to existing TNGF and N3IWF shall be analyzed before any conclusion on WT#3.

NOTE: Coordination with BBF and CableLabs will take place as needed during the study.

# 5 Key Issues

## 5.1 Key Issues for DualSteer

### 5.1.1 Key Issue #1.1: Subscription aspects to support DualSteer

#### 5.1.1.1 Description

This key issue will study the enhancements of subscription aspects to support DualSteer including the following:

- Whether and how the 5G System identifies and associates the two subscriptions/SUPIs for DualSteer.

- Whether it is needed and what enhancements are required in the policy subscription data to support generation of rules/policies for DualSteer.

- Whether it is needed and what enhancements are required in subscription data to support Registration and Mobility Management and management of PDU sessions for DualSteer.

### 5.1.2 Key Issue #1.2: Registration and mobility management for DualSteer

#### 5.1.2.1 Description

This Key Issue will study the overall registration and mobility management impacts to support DualSteer including the following:

- Whether and what enhancements are needed in functions and procedures of registration, deregistration and mobility management for supporting DualSteer.

### 5.1.3 Key Issue #1.3: Session management aspects for DualSteer

#### 5.1.3.1 Description

This key issue will study the following potential session management enhancements to support DualSteer:

- Whether and how to enhance session management functions and procedures for DualSteer traffic steering of a new service to a 3GPP access network and/or the DualSteer traffic switching across two 3GPP access networks belonging to the same PLMN (either HPLMN or VPLMN) or two different PLMNs or PLMN and PNI-NPN, which may further include the following:

- Whether and what enhancements are required in PDU Session establishment/modification/release;

- Whether and what enhancements are required for N4 session management between the SMF and UPF, or between SMF+PGW-C and UPF+PGW-U; and

- For session subject to potential switching and/or to traffic steering, whether, when and how the network selects the PSA UPF(s) or UPF+PGW-U to allow routing the traffic across 3GPP access networks towards the same PSA UPF or UPF+PGW-U to support DualSteer.

NOTE: Impact to existing session management functionality related to the move of a service-related data between a 3GPP access network and a non-3GPP access network will be considered as part of this key issue.

### 5.1.4 Key Issue #1.4: Policy enhancements for DualSteer

#### 5.1.4.1 Description

This key issue aims to study whether and how to define the policies by the HPLMN to support DualSteer traffic steering and/or DualSteer traffic switching:

- Whether and what policies need to be provided by the HPLMN to guide the DualSteer device to decide to connect to an additional PLMN/PNI-NPN, or an additional 3GPP access network within the same PLMN;

- For DualSteer traffic steering, whether and what policies need to be provided by the HPLMN to guide the DualSteer device to select a 3GPP access network to be used for the new service;

- For DualSteer traffic switching, whether and what policies need to be provided by the HPLMN to guide the DualSteer device for traffic switching between two connected 3GPP access networks;

- Whether and what policies are provided within the network(s) to handle DualSteer traffic steering and/or DualSteer traffic switching;

- Study whether and how the policy enhancements for DualSteer device have impacts on existing UE policies.

NOTE: Impact to existing policy management functionality related to the move of a service-related data between a 3GPP access network and a non-3GPP access network will be considered as part of this key issue.

## 5.2 Key Issues for ATSSS\_Ph4

### 5.2.1 Key Issue #2.1: MPQUIC steering functionality to steer, switch and split non-UDP traffic

#### 5.2.1.1 Description

Currently MPQUIC steering functionality can support steering, switching, and splitting of UDP traffic based on IETF protocols, using UDP proxying over HTTP. For TCP traffic, ATSSS has been relying on the use of the "MPTCP steering functionality" that was specified in Rel-16. The associated proxy functionalities (MPQUIC and MPTCP) add complexity for the operator deployment. In order to ease this deployment burden, it needs to be studied how to enable the MPQUIC steering functionality to also steer, switch, and split non-UDP traffic (i.e. TCP, IP and Ethernet traffic) and at the same time make the MPTCP steering functionality optional for TCP traffic in ATSSS.

In order to support MPQUIC steering functionality to steer, switch, and split non-UDP traffic (i.e. TCP, IP, Ethernet traffic) the following aspects need to be studied:

- What enhancements are required to existing Rel-18 MPQUIC steering functionality described in TS 23.501 [3] to support proxying of TCP traffic using MPQUIC;

- What enhancements are required to existing Rel-18 MPQUIC steering functionality to support proxying of general IP traffic using MPQUIC;

- What enhancements are required to existing Rel-18 MPQUIC steering functionality to support proxying of Ethernet traffic using MPQUIC.

Solutions need to be based on IETF protocols.

Any new ATSSS capabilities specified for UE would be applicable for ATSSS-capable 5G-RGs, if endorsed by BBF and/or CableLabs; FN-RG are not in the scope of the study.

### 5.2.2 Key Issue #2.2: Simplified ATSSS architecture over non-3GPP access

#### 5.2.2.1 Description

The current ATSSS architecture requires that non-3GPP access is provided via the trusted or untrusted non-3GPP access procedures. This means that to enable ATSSS either a TNGF or an N3IWF is deployed. This key issue studies whether and how to define a functional architecture and procedures for steering, switching, and splitting of traffic not utilising the TNGF/N3IWF as specified in Rel-18 and earlier releases (TS 23.501 [3]) to simplify the network operation over non-3GPP access, without compromising the security of the 5G network. In particular, this key issue studies the following issues:

1) Protocol stack simplification

- Whether and how to eliminate the NAS signalling connection over non-3GPP access, or not.

- Whether and how to eliminate IPSec tunnel encapsulation on the user plane only or both on the control plane and the user plane, in order to simplify the UE protocol stack and reduce the user plane overhead.

2) "non-3GPP access without 5G NAS over non-3GPP".

- Whether and how to support splitting, switching, steering between 3GPP access and "non-3GPP access without 5G NAS over non-3GPP".

- Whether and how to enhance registration and security aspects for supporting "non-3GPP access without 5G NAS over non-3GPP". This may include studying also whether registration would be used over non-3GPP access.

NOTE: During the study on this KI, consultation with SA WG3 is needed for handling security aspects.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of DualSteer Solutions to Key Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Key Issues for DualSteer | | | |
| Solution# | <Key Issue #1.1> | <Key Issue #1.2> | <Key Issue #1.3> | <Key Issue #1.4> |
| #X |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 6.0-2: Mapping of ATSSS\_Ph4 Solutions to Key Issues

|  |  |  |
| --- | --- | --- |
|  | Key Issues for ATSSS\_Ph4 | |
| Solution# | <Key Issue #2.1> | <Key Issue #2.2> |
| #2.1 | **X** |  |
| #2.2 |  | **X** |
| #2.3 | **X** |  |
| #2.4 | **X** |  |
| #2.5 | **X** |  |
| #2.6 |  | **X** |
| #2.7 |  | **X** |
| #2.8 |  | **X** |

## 6.1 Solutions for DualSteer

### 6.1.X Solution #X: <Solution Title>

#### 6.1.X.1 Description

Editor's note: This clause will describe the solution principles and architecture assumptions for corresponding key issue(s). (Sub) clause(s) may be added to capture details.

#### 6.1.X.2 Procedures

Editor's note: This clause describes high-level procedures and information flows for the solution.

#### 6.1.X.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing 3GPP services, entities and interfaces.

## 6.2 Solutions for ATSSS\_Ph4

### 6.2.1 Solution #2.1: Policy Control for the MPQUIC Steering Functionality for non-UDP Traffic

#### 6.2.1.1 Description

The MPQUIC steering functionality can be enhanced to enable different CONNECT protocols to be used (i.e., with protocol values connect-udp [6], connect-ip [7], connect-ethernet [8]), possibly concurrently in the same PDU session. Furthermore, at least one of these CONNECT protocols also supports associated parameters (connect-ip supports target and ipproto parameters defined in RFC 9484 [7]).

The network operator should be able to influence the type of CONNECT protocol and applicable associated parameters used for a flow when using the MPQUIC steering functionality. In this proposed solution, the operator configures the desired protocol and parameters in a policy rule. In some cases, multiple protocols may be configured for a flow, in which case the UE needs to select an appropriate protocol among the allowed ones.

The MA PDU session control information of a PCC rule is extended to include allowed CONNECT protocol(s) and the values of related parameters. When an SMF selects the MPQUIC steering functionality for a flow, it determines the allowed CONNECT protocol(s) and values of related parameters, using this information. The SMF sends the allowed CONNECT protocol(s) and values of related parameters both to the UPF (MAR over N4) and to the UE (ATSSS rule in the PDU session establishment or update accept). The UPF uses the allowed protocols and parameter values to configure the MPQUIC proxy, e.g., to accept only the allowed protocols and parameter values. The UE uses the allowed protocols and parameter values to determine how to setup the MASQUE session. If a single CONNECT protocol is allowed, the UE uses this protocol in the CONNECT request. If multiple CONNECT protocols are allowed, the UE determines which protocol to use in the request (for example, using the application protocol and PDU session type). For example, if the application protocol is over UDP, and the PDU session type is IP, the UE may select the connect-udp or connect-ip protocol if they are both allowed by the network. In another example, if the PDU session type is Ethernet, the UE may select the connect-ethernet protocol.

#### 6.2.1.2 Procedure



Figure 6.2.1.2-1: Policy-Controlled MA PDU Session using MPQUIC Steering Mode for Non-UDP Traffic

The above Figure 6.2.1.2-1 shows how the CONNECT protocol and values of related parameters are selected over an MA PDU Session using the MPQUIC steering functionality.

0. Policy rules that include allowed CONNECT protocol(s) and values of related parameters are provisioned in the network. The provisioning is similar to other existing MA PDU Session Control information such as the Transport Mode for MPQUIC steering functionality. It may be based on preference from the AF.

NOTE: How the 5GC obtains AF preference is out of SA2 scope.

1. A UE application triggers the establishment of a new application flow.

2. The UE sends an MA PDU session establishment or update request to the SMF.

3. The SMF requests a policy control update from the PCF.

4. The PCF sends PCC rule(s) to the SMF. The MA PDU Session control information in the PCC rules can include a set of allowed CONNECT protocols. Additional parameters associated with a connect protocol, if applicable, may also be provided. For example, t "ipproto" and "target" parameters associated with CONNECT-IP [7] can be provided.

5. The SMF determines to use the MPQUIC steering function and steering mode based on PCC rule(s).

6. The SMF configures the N4 session in UPF and passes the allowed CONNECT protocol(s) and values of related parameters in MAR to the UPF (as well as steering functionality, steering mode and other ATSSS related parameters).

7. The UPF configures the MPQUIC proxy using the allowed CONNECT protocol(s) and values of related parameters to the UPF.

8. The UPF sends a response to the SMF.

9. The SMF sends a PDU session establishment/update response to the UE, including an ATSSS rule with the allowed CONNECT protocol(s) and values of related parameters.

10. The UE selects a CONNECT protocol appropriate for the application flow, as well as the values of related parameters. according to the received ATSSS rules. If multiple CONNECT protocols are allowed in the ATSSS rules, the selection is up to UE implementation.

11. The UE selects an MPQUIC connection corresponding to the service data flow’s MA PDU session and QoS flow, if it exists. Otherwise, the UE establishes a new MPQUIC connection with the MPQUIC proxy on the UPF.

12. The UE sends a CONNECT request on the selected MPQUIC connection. The CONNECT request includes the selected CONNECT protocol and values of related parameters.

13. The UPF enforces that the request corresponds to the allowed CONNECT protocol(s) and values of related parameters.

14. The UPF sends a response to the CONNECT request.

15. If needed, the UE can establish the second leg of the MA PDU session, over another access.

From this point on, the UE and UPF select access to send UL and DL PDUs, based on the steering mode, over the MASQUE connection between UE and UPF, associated to the CONNECT request.

#### 6.2.1.3 Impacts on services, entities and interfaces

UE:

- Select the CONNECT protocol and values of related parameters to use in the CONNECT request (based on ATSSS rules from the SMF including allowed CONNECT protocol(s) and values of related parameters).

PCF, UDM:

- MA PDU session control information in PCC rules can include allowed CONNECT protocol(s) and values of related parameters

SMF:

- Determine the allowed CONNECT protocol(s) and values of related parameters and provide this information to the UPF and the UE.

UPF:

- The MPQUIC proxy additionally supports connect-ip and connect-ethernet services.

- Configure the MPQUIC proxy to accept the CONNECT requests with allowed CONNECT protocol(s) and values of related parameters.

### 6.2.2 Solution #2.2: IPsec establishment using null encryption with ePDG co-located in the UPF

#### 6.2.2.1 Description

This solution addresses key issue #2.2.

This solution basically re-use the existing ePDG architecture/functionality, which means the ePDG is co-located with the PSA UPF. Figure 6.2.2.1-1 shows overall architecture of this solution. When a UE establishes MA PDU Session over 3GPP access, the SMF+PGW-C, based on interaction with PSA UPF, provides ePDG information to be used over non-3GPP access to the UE. If the UE receives the ePDG information, the UE triggers attach procedure towards ePDG/5GC using the existing procedure, which results in authentication of UE and adding non-3GPP access path to the established MA PDU Session. During the procedure, UE/ePDG uses null encryption to avoid duplicated encryption.



Figure 6.2.2.1-1: Overall architecture

#### 6.2.2.2 Procedures



Figure 6.2.2.2-1: MA PDU Session Establishment using ePDG co-located in the UPF

1. A UE registers over 3GPP access.

2. The UE sends PDU Session Establishment Request to establish a MA PDU Session. In the request message, the UE indicates that the UE support simplified ATSSS architecture over non-3GPP access.

3. Based on the simplified ATSSS architecture support indication, the SMF+PGW-C requests the PSA UPF to allocate ePDG address to be used for the MA PDU Session.

4. The SMF+PGW-C provides ePDG information to the UE in the PDU Session Establishment Accept message.

5. The SMF+PGW-C registers the MA PDU Session to the HSS/UDM.

6. The UE connects to the ePDG based on ePDG information received in step 4 and triggers initial attach procedure. During the procedure, in the IKE signalling, the UE includes PDU Session ID and IP address of the MA PDU Session established over 3GPP access and necessary information for MA PDU Session as described in clause 4.22.2.4.2 of TS 23.502 [x]. When the ePDG and the UE negotiate encryption algorithm, null encryption is selected.

7. If authentication is successful, the ePDG sends Create Session Request and the SMF+PGW-C sends Create Session Response. This triggers the ePDG to create internal tunnel between the ePDG and PSA UPF. How the internal tunnel is created is not in the scope of this solution and depends on implementation.

8. The IKEv2 signalling is sent to the UE to notify successful addition of access leg to the existing MA PDU Session.

#### 6.2.2.3 Impacts on services, entities and interfaces

UE:

- includes capability of simplified ATSSS architecture over non-3GPP access during the PDU Session Establishment Request procedure.

- based on received ePDG information during the MA PDU Session establishment, connects to the ePDG and triggers initial attach procedure.

SMF+PGW-C:

- based on UE capability, requests to allocate ePDG address to the UPF and sends the ePDG information to the UE in the PDU Session Establishment Accept.

UPF:

- based on SMF+PGW-C requests, allocates ePDG address to be used simplified ATSSS architecture over non-3GPP access.

### 6.2.3 Solution #2.3: MPQUIC Steering Functionality extended with additional CONNECT methods

#### 6.2.3.1 Description

This solution addresses KI#2.1.

The Rel-18 MPQUIC functionality enables steering, switching, and splitting of UDP traffic between the UE and UPF, in accordance with the ATSSS policy created by the network. The operation of the MPQUIC functionality is based on RFC 9298 [6] "proxying UDP in HTTP", which specifies how UDP traffic can be transferred between a client (UE) and a proxy (UPF) using the RFC 9114 [9] HTTP/3 protocol.

To enable this functionality, the SMF indicates the proxy type that is required (CONNECT-UDP in case of MPQUIC) and the UPF provides the require information back to SMF (e.g. MPQUIC proxy IP address and port). The SMF then sends MPQUIC proxy information to UE, i.e. one IP address of UPF, one UDP port number and also indicates the proxy type (currently only "connect-udp" is supported for MPQUIC). This information is used by the UE for establishing multipath QUIC connections with the UPF, which implements the MPQUIC Proxy functionality. The CONNECT-UDP proxy method is defined in RFC 9298.

To enhance the MPQUIC solution to support proxying IP, TCP and Ethernet, this solution proposes that the following IETF specifications are used:

- CONNECT-IP as defined in RFC 9484 [7]. This RFC describes how IP packets can be transferred between a client (UE) and a proxy (UPF) using the RFC 9114 [9] HTTP/3 protocol over MPQUIC.

- CONNECT-TCP as updated by IETF WG Internet Draft draft-ietf-httpbis-connect-tcp [10]. This I-D describes an alternative proxy solution for TCP that is similar to CONNECT-UDP and CONNECT-IP and works with HTTP/3 over QUIC and UDP. This proxy solution for TCP is thus required in order to fit into the existing rel-18 MPQUIC solution in order to proxy TCP traffic.

- CONNECT-Ethernet as described in IETF WG Internet Draft draft-ietf-masque-connect-ethernet [8]. This I-D describes how to proxy Ethernet frames in HTTP.

NOTE: The use of the IETF solutions for TCP proxying and Ethernet proxying is dependent on the IETF drafts being stable in time for Rel-19.

CONNECT-IP, CONNECT-UDP and CONNECT-TCP can be used with IP based PDU Session types (IPv4, IPv6, IPv4v6) while CONNECT-Ethernet can be used with Ethernet PDU Session type.

#### 6.2.3.2 HTTP CONNECT methods

Proxy UDP (connect-udp):

- Proxying of UDP traffic is based on RFC 9298 [6] supporting proxy of UDP traffic in HTTP/3. The UDP Proxying Payload contains the payload of a UDP packet. The proxied UDP payload is encapsulated in HTTP/3 datagrams [11].

Proxy TCP (connect-tcp):

- draft-ietf-httpbis-connect-tcp [10] defines an updated HTTP CONNECT method for TCP based on a similar approach as connect-udp. The TCP Proxying Payload contains the payload of a TCP packet. HTTP/3 datagram format is not required since TCP is a stream-based protocol and the MPQUIC proxy reads bytes from the incoming stream and inserts into the outgoing stream.

Editor's note: Further description and analysis of CONNECT-TCP is FFS, e.g. related to performance aspects and how TCP traffic is proxied over MPQUIC.

Proxy IP (connect-ip):

- RFC 9484 [7] allows proxying of arbitrary IP packets. It allows an HTTP client to create an IP tunnel through an HTTP/3 server that acts as an IP proxy. The proxied IP packets, including the IP header, are encapsulated in HTTP/3 datagrams [11].

Proxy Ethernet (connect-ethernet):

- draft-ietf-masque-connect-ethernet [8], describes proxying of Ethernet frames over HTTP/3. The proxied Ethernet frames are encapsulated in HTTP/3 datagrams [11].

#### 6.2.3.2 Procedures

##### 6.2.3.2.1 MA PDU Session Establishment



Figure 6.2.3.2-1: PDU Session Establishment

1. The UE sends a PDU Session Establishment Request message and includes the ATSSS capabilities as per rel-18. In addition, if the UE supports MPQUIC with other proxy protocols than connect-udp and in case of IP-based PDU Session types, the UE includes the supported MPQUIC proxy protocols (connect-ip, connect-udp and/or connect-tcp) as part of the SM NAS message.

NOTE 1: In case of Ethernet PDU Session type, it is assumed that a UE supporting MPQUIC also supports the connect-ethernet proxy protocol, i.e. there is no need to explicitly signal the support for connect-ethernet.

2. The AMF selects and SMF and sends a Nsmf\_PDUSession\_Create Request message with the PDU Session Establishment Request message.

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 is configured, as part of the DNN configuration, what proxy protocols are supported. For example, a specific DNN may support connect-tcp and connect-udp but not connect-ip.

NOTE 2: The DNN configuration on the SMF may e.g. indicate that connect-ip is supported, or that connect-udp and connect-tcp are supported, depending on the use case and operator configuration.

The SMF selects a UPF that supports the proxy protocols required, if possible. The SMF may discover the UPF capabilities via NRF or the N4 Association Establishment.

6. 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 (e.g. ATSSS\_LL and/or MPQUIC). In addition, for IP based PDU Session types, the SMF also includes the required MPQUIC proxy protocols (connect-ip, connect-udp, and/or connect-tcp). For Ethernet PDU Sessions there is no need to explicitly indicate proxy protocol, but it may be done to keep stage 3 aligned between PDU Session Types.

If the message from SMF instructs the UPF to activate MPQUIC functionality, the UPF allocates MPQUIC proxy information (IP address and port of the MPQUIC proxy in UPF), as specified for rel-18.

If the message from the SMF instructs the UPF to activate MPQUIC functionality, the UPF also allocates the UE "MPQUIC link-specific multipath" addresses/prefixes and provides these to SMF, as per rel-18. The UPF only allocates a single set of UE "MPQUIC link-specific multipath" addresses/prefixes for MPQUIC, independent of the proxy protocols used.

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

7. The SMF triggers SM Policy Association Establishment and indicates with the MA PDU Session capabilities what traffic types are supported for MPQUIC. This allows the PCF to create PCC rules with MPQUIC support for other traffic than UDP.

8-9. The SMF sends the PDU Session Establishment Accept to the UE and includes the MPQUIC proxy information (i.e. the IP address, a port number) In case of IP based PDU Session types, the SMF also indicates the type of the MPQUIC proxy/proxies supported for the MA PDU Session). The SMF also provides the UE "MPQUIC link-specific multipath" addresses/prefixes.

10. The MA PDU Session Establishment is completed, as described in TS 23.502 [4].

After the PDU Session establishment, in case MPQUIC steering functionality is to be used for a specific traffic flow according to the ATSSS rules, the UE selects a proxy protocol based on the application type (e.g. UDP or TCP) and the supported proxy methods. In case multiple proxy methods are supported for a specific traffic flow (e.g. for a UDP based traffic flow, if both connect-ip and connect-udp are supported for the MA PDU Session) the UE selection of proxy method is UE implementation specific.

##### 6.2.3.2.2 PDN Connections and Multi Access PDU Sessions

When the UE wants to request a new PDN Connection in 3GPP access in EPC and wants to use this PDN Connection as user-plane resource associated with a MA PDU Session, the PDN Connection procedure as defined in TS 23.502 [3], clause 4.22.2.3.2, is used with the following differences:

- If the UE supports MPQUIC with other proxy protocols than connect-udp and in case of IP-based PDU Session types, the UE includes in the PCO the supported MPQUIC proxy protocols (connect-ip, connect-udp and/or connect-tcp).

- The PGW-C+SMF selects UPF and triggers SM policy association establishment as described in clause 6.2.3.2.1, steps 5-7.

- The PGW-C+SMF provides via the PCO in the Create Session Response message to the UE the MPQUIC proxy protocols allowed for the MA PDU Session.

When the UE wants to request a new PDN Connection in non-3GPP access in EPC and wants to use this PDN Connection as user-plane resource associated with a MA PDU Session, the PDN Connection procedure as defined in TS 23.502 [3], clause 4.22.2.4.2, is used with the following differences:

- If the UE supports MPQUIC with other proxy protocols than connect-udp and in case of IP-based PDU Session types, the UE includes in the IKE signalling to ePDG the supported MPQUIC proxy protocols (connect-ip, connect-udp and/or connect-tcp). The ePDG forwards the information via APCO in the Create Session Request.

- The PGW-C+SMF selects UPF and triggers SM policy association establishment as described in clause 6.2.3.2.1, steps 5-7.

- The PGW-C+SMF provides via the APCO in the Create Session Response message to the UE the MPQUIC proxy protocols allowed for the MA PDU Session. The ePDG forwards the information to the UE via IKE signalling.

#### 6.2.3.3 Impacts on services, entities and interfaces

UE:

- Support for additional MPQUIC proxy protocols.

- SM NAS enhancements to negotiate the support for additional MPQUIC proxy protocols (enhanced 5GSM capability, enhanced ATSSS container).

- IKEv2 enhancements to negotiate the support for additional MPQUIC proxy protocols (enhanced 5GSM capability, enhanced ATSSS container).

SMF:

- SM NAS and PCO enhancements to negotiate the support for additional MPQUIC proxy protocols (enhanced 5GSM capability, enhanced ATSSS container).

- N4 enhancements to instruct UPF to use additional MPQUIC proxy protocols.

UPF:

- Support for additional MPQUIC proxy protocols.

- N4 enhancements to activate the use of additional MPQUIC proxy protocols.

PCF:

- Take into account additional MA PDU Session capabilities to support MPQUIC also for TCP, IP and Ethernet traffic flows.

ePDG:

- IKEv2 and APCO enhancements to negotiate the support for additional MPQUIC proxy protocols (enhanced 5GSM capability, enhanced ATSSS container).

No impacts to AMF, UDM.

No impacts to ATSSS rules.

### 6.2.4 Solution #2.4: MPQUIC steering functionality using IP proxying over HTTP

#### 6.2.4.1 Introduction

The solution in this clause specifies a new ATSSS steering functionality, called Multipath QUIC-IP (MPQUIC-IP) steering functionality, and addresses the objective of KI#2.1 for a QUIC-based steering functionality to allow the transport of IP packets over multiple accesses between UE and UPF. It generalizes on the current solution for ATSSS Phase 3 [17] for proxying UDP packets over HTTP over MP QUIC and extends it to generic IP traffic.

The solution is primarily based on the RFC 9484 [7], which specifies how IP traffic can be transferred between a client (UE) and a proxy (UPF) using the HTTP/3 protocol [9]. The HTTP/3 protocol operates on top of the QUIC protocol [12], which supports simultaneous communication over multiple paths, as defined in draft-ietf-quic-multipath [16].

The solution considers the following modes for transmitting an IP flow (see further details in clause 6.2.4.3, step 5):

- Datagram mode 1: This mode encapsulates the IP packets into QUIC DATAGRAM frames. It provides unreliable transport and adds sequence numbers to the transmitted IP packets, so that the received IP packets can be re-ordered, and the duplicated IP packets can be removed.

- Datagram mode 2: This mode encapsulates the IP packets into QUIC DATAGRAM frames. It provides unreliable transport but does not add sequence numbers to the transmitted IP packets. Therefore, it may result in data delivery with out-of-order packets and/or with duplicated packets.

- Stream mode: This mode encapsulates the IP packets into QUIC STREAM frames. It provides reliable transport (based on the existing mechanisms supported by the QUIC protocol) and supports data delivery without out-of-order packets and without duplicated packets.

Editor’s note: How this solution interacts with other "connect-x" based solutions to completely fulfil the scope of the KI #2.1 is FFS.

#### 6.2.4.2 High-level Description

The key principles of the solution are summarized below.

- After the MA PDU Session establishment, the UE creates one or more multipath QUIC connections with the UPF. Each multipath QUIC connection is associated with a QoS flow, i.e. it carries the traffic mapped to a QoS flow.

- The UE operates as a connect-ip client and the UPF operates as a connect-ip proxy, both defined in RFC 9484 [7]. Therefore, the UE supports an HTTP/3 client and the UPF supports an HTTP/3 proxy, both of them operating over QUIC.

- On each of the established QUIC connections, the UE sends an extended HTTP CONNECT request to UPF (as defined in [9]) indicating that IP proxying over HTTP is needed.

- When the UE wants to transmit an uplink packet of an IP flow, the UE:

- Selects which QUIC connection will be used for the uplink traffic of the IP flow based on the QoS flow associated with the IP flow;

- Creates a new bidirectional QUIC stream on the selected QUIC connection;

- Configures the QUIC stream to apply a steering mode (i.e. the steering mode that should be used for the uplink traffic of the IP flow based on the ATSSS rules); and

- Forwards to UPF the uplink packets of the IP flow using multipath QUIC transport.

- When the UPF wants to transmit a downlink packet of an IP flow, the UPF:

- Selects which QUIC connection will be used for the downlink traffic of the IP flow (this QUIC connection is the same as the one selected by UE for the IP flow, assuming the QoS flow in UL and DL directions is the same);

- Selects a bidirectional QUIC stream on the selected QUIC connection (this QUIC stream is the same as the one created by the UE for the IP flow);

- Configures the QUIC stream to apply a steering mode (i.e. the steering mode that should be used for the downlink traffic of the IP flow based on the N4 rules); and

- Forwards to UE the downlink packets of the IP flow using multipath QUIC transport.

The following figure illustrates how the traffic of an IP flow is transferred between the UE and UPF using multipath QUIC transport. In this figure, it is assumed that the uplink traffic and the downlink traffic of the IP flow are mapped to the same QoS flow (QFI-1). Therefore, both the uplink traffic and the downlink traffic of the IP flow use the same multipath QUIC connection.



Figure 6.2.4.2-1: Using multipath QUIC transport for a IP flow

The bidirectional QUIC stream is established by the UE to enable transmission of uplink IP packets (blue) and downlink IP packets (red) of the IP flow. The UE configures this stream to send uplink traffic with a steering mode determined based on the ATSSS rules in the UE (uplink steering mode). The UPF configures this stream to send downlink traffic with a steering mode determined based on the N4 rules in the UPF (downlink steering mode). The data packets of the IP flow shown in Fig. 6.2.4.2-1 are transmitted in datagram mode (mode 1 or mode 2), i.e. they are encapsulated in HTTP datagrams and QUIC DATAGRAM frames, each one carrying header information (see the Quarter Stream ID defined in RFC 9114 [9]) that associates it with the established bidirectional stream. As discussed below, the IP packets of the IP flow may be transmitted in stream mode (instead of datagram mode), i.e. transmitted directly over the bidirectional stream. In this case, the IP packets of the IP flow are encapsulated in DATAGRAM capsules and QUIC STREAM frames.

Figure 6.2.4.2-2 and Figure 6.2.4.2-3 illustrate the components of the MPQUIC-IP steering functionality used to support data transmission in the uplink and downlink direction respectively. The MPQUIC-IP steering functionality is composed of three components:

1) QoS flow selection & Steering mode selection: This component in the UE initiates the establishment of one or more QUIC connections, after the establishment of the MA PDU Session and, for each uplink IP flow, it selects a QoS flow (based on the QoS rules), a steering mode (based on the ATSSS rules) and a transport mode (see further details below). This component in the UPF selects, for each downlink IP flow, a QoS flow (based on the N4 rules), a steering mode (based on the N4 rules) and a transport mode (see further details below).

In the UE, this component is only used in the uplink direction, while, in the UPF, this component is only used in the downlink direction.

2) HTTP/3 layer: Supports the HTTP/3 protocol defined in RFC 9114 [9] and the extensions defined in:

- RFC 9484 [7] for supporting IP proxying over HTTP; and

- RFC 9297 [11] for supporting HTTP datagrams.

The HTTP/3 layer selects a QUIC connection to be used for each IP flow and allocates a new QUIC stream on this connection that is associated with the IP flow. It also configures this QUIC stream to apply a specific steering mode (further details are provided below).

In the UE, the HTTP/3 layer implements an HTTP/3 client, while, in the UPF, it implements an HTTP/3 proxy.

3) QUIC layer: Supports the QUIC protocol as defined in the applicable IETF specifications (RFC 9000 [12], RFC 9369 [18], RFC 9001 [13], RFC 9002 [14]) and the extensions defined in:

- RFC 9221 [15] for supporting unreliable datagram transport with QUIC; and

- draft-ietf-quic-multipath [16] for supporting QUIC connections using multiple paths simultaneously.



Figure 6.2.4.2-2: Components of MPQUIC-IP steering functionality used for UL data transmission



Figure 6.2.4.2-3: Components of MPQUIC-IP steering functionality used for DL data transmission

The protocol stack of the solution is depicted in Figure 6.2.4.2-4 below.



Figure 6.2.4.2-4: UP protocol stack of the solution

#### 6.2.4.3 Procedures

Figure 6.2.4.3-1 below depicts the key steps of the procedure that enables data traffic to be exchanged between the UE and UPF using the MPQUIC-IP steering functionality.



Figure 6.2.4.3-1: Procedure for enabling data traffic using the MPQUIC-IP steering functionality

1. The UE establishes a MA PDU Session with the 5G core (5GC) network. During the MA PDU Session establishment:

- In the PDU Establishment Request message, the UE indicates that it supports the MPQUIC-IP steering functionality. This indication can be used by the network (a) to select a UPF that also supports the MPQUIC-IP steering functionality and (b) to decide whether the ATSSS/N4 rules for the MA PDU Session may use the MPQUIC-IP steering functionality.

- The UE receives MPQUIC-IP proxy information, i.e. one IP address of UPF, one UDP port number and the proxy type (e.g. "connect-ip"). This information is used by the UE for establishing QUIC connections with the UPF, which is also referred to as "MPQUIC-IP proxy".

- The UE receives one IP address/prefix for the MA PDU Session and two additional IP addresses/prefixes, called "link-specific multipath QUIC" addresses; one associated with 3GPP access and another associated with the non-3GPP access. These two addresses can be used by the UE to create two paths in a multipath QUIC connection.

- The UE receives QoS rules and ATSSS rules to be applied for the MA PDU Session, for QoS enforcement and traffic steering enforcement respectively. Similar rules (N4 rules) are received by UPF.

2. After the MA PDU Session is established and the UE identifies that one or more ATSSS rules require traffic steering using the MPQUIC-IP steering functionality, the UE determines the number of multipath QUIC connections to be established with the UPF (MPQUIC-IP proxy). For example, the UE may determine to establish 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. The QoS rules provided to UE include downlink QoS information and the UE applies the downlink QoS information to establish QUIC connections for the QoS flows used for downlink traffic only.

3. The UE establishes the number of multipath QUIC connection with the UPF (MPQUIC-IP proxy) determined in the previous step. This results into several multipath QUIC connections between the UE and UPF, each one composed of multiple paths, e.g. one path over 3GPP access and another path over non-3GPP access. Data transmitted over a multipath QUIC connection must be encrypted according to RFC 9001 [13].

During a QUIC connection establishment, the UE and UPF negotiate QUIC transport parameters and indicate (a) support of QUIC Datagram frames and (b) support of multipath. They indicate support of QUIC Datagram frames by providing the "max\_datagram\_frame\_size" transport parameter with a non-zero value (see RFC 9221 [15]) and they indicate support of multipath by providing the "enable\_multipath" transport parameter (see draft-ietf-quic-multipath [16]).

After a QUIC connection establishment, the HTTP/3 client and the HTTP/3 proxy negotiate HTTP settings and indicate support of HTTP Datagrams (see RFC 9297 [11]) and support of Extended CONNECT (see RFC 9220 [19]).

The QoS flow associated with a QUIC connection is also negotiated between the UE and UPF. This is done by using a new QUIC transport parameter (defined by 3GPP) when the QUIC connection is established.

NOTE 1: QUIC transport parameter needs to be registered in IANA (by stage 3).

4. On each of the established QUIC connections, the UE may either send an extended HTTP CONNECT request to UPF (as defined in RFC 9484 [7]) immediately after a multipath QUIC connection is created (as a proactive action), or when the UE allocates a new QUIC stream from the multipath QUIC connection (e.g. based on QFI). This extended HTTP CONNECT request, essentially indicates that IP proxying over HTTP is needed. If this is accepted by UPF, it responds with a 200 status.

5. The UE generates a new IP packet (IP packet #1) that should be sent via the MA PDU Session. This IP packet initiates a new IP flow, i.e. a sequence of IP packets using the same 5-tuple. For this new IP flow (and for each new IP flow):

- The UE selects a QoS flow (QFI) over which the IP flow should be transmitted. This is selected by using the received QoS rules.

- The UE selects a steering mode that should be applied for the IP flow. This is selected by using the received ATSSS rules.

- The UE selects a transport mode, e.g. a datagram transport mode or the stream transport mode. This is selected by using the received ATSSS rules, i.e. each ATSSS rule which indicates that the MPQUIC-IP steering functionality should be applied for the matching traffic, indicates also the transport mode that should be applied for this traffic.

The datagram transport mode supports the following two sub-modes of operation:

- Datagram mode 1 (with sequence numbers): The HTTP/3 proxy/client or the "QoS flow selection and Steering mode selection" layer prefixes each UDP data with a sequence number before passing it to the QUIC layer for multipath transmission. The sequence numbers are applied by the receiving endpoint to re-order the UDP data and remove duplicated UDP data.

- Datagram mode 2 (without sequence numbers): The HTTP/3 proxy/client does not prefix each IP packet with a sequence number before passing it to the QUIC layer for multipath transmission. This may result (depending on the applied steering mode) in data delivery with out-of-order packets and/or with duplicated packets. For some applications, however, such type of data delivery may be acceptable.

The datagram mode 2 is needed (although it does not support re-ordering) because it features benefits compared to ATSSS-LL, e.g. (a) it supports congestion control, (b) it supports RTT/PLR measurements without the need to implement the PMF protocol, etc.

In both datagram modes, every IP packet is encapsulated within an HTTP DATAGRAM, which if further encapsulated within an QUIC DATAGRAM frame [15]. The payload of the HTTP DATAGRAM is composed of a Context ID and a Payload (as defined in RFC 9484 [7]): HTTP DATAGRAM payload = {Context ID (i), Payload (..)}.

The Datagram mode 1 and Datagram mode 2 use two different (and pre-defined in 3GPP) Context IDs, e.g. Context ID=0 and Context ID=1, respectively. With Context ID=0, the Payload contains the IP packet, whereas, with Context ID=1, the Payload contains a sequence number followed by the IP packet. The format of QUIC DATAGRAMs used in both datagram modes is shown below. The Datagram mode 1 may support reordering either in the HTTP/3 layer (as described above) or in the layer above HTTP/3. In the latter case, the definition of a new Context ID is not needed as sequencing and reordering is performed outside the HTTP/3 layer.

6. The UE selects a multipath QUIC connection to be used for the new IP flow (e.g. based on the selected QFI).

Editor’s note: It is FFS how different steering modes can be applied for different IP flows, which are transmitted in the same IP tunnel between the UE and UPF.

7. The UE sends the IP packet using the allocated new stream on the selected QUIC connection.

When the datagram transport mode is selected (mode 1 or mode 2), the UE encapsulates the IP packet within an HTTP DATAGRAM frame, which is transferred inside a QUIC DATAGRAM frame. The header of the HTTP DATAGRAM indicates that this datagram is associated with stream 40 (i.e. the Quarter Stream ID is set to 10).

When the stream transport mode is selected, the UE encapsulates the IP packet within an HTTP DATAGRAM frame that is further encapsulated in a DATAGRAM capsule, which is transferred inside a QUIC STREAM frame.

In the example procedure shown in Figure 6.2.4.3-1, the datagram transport mode (mode 1 or mode 2) is selected. The UE sends a QUIC DATAGRAM frame to UPF that encapsulates the IP packet, which is forwarded by UPF to the remote host.

8. When an IP packet is received by UPF (MPQUIC-IP proxy) from the remote host (IP packet #2), this IP packet is transferred to the UE using the established context information for the IP flow, i.e. using the selected multipath QUIC connection, the selected stream on this connection, the selected steering mode, and the selected transport mode. Such context information is stored in the UPF and in the UE and is applied for all the IP packets of the IP flow.

9. Similarly, when another IP packet is generated by the UE app (IP packet #3), this IP packet is transferred to UPF (MPQUIC-IP proxy) using again all the stored context information for the IP flow.

NOTE 2: The context information for an IP flow in the UE and in the UPF is created when the initial IP packet (i.e. IP packet #1) of this IP flow is transferred. All subsequent IP packets of the same IP flow are transferred between the UE and the UPF using this context information.

When the UE identifies that the context information for an IP flow is no longer needed, the UE deletes this context information and releases the associated QUIC stream, which cause the UPF to delete the context information stored in UPF.

The following figure 6.2.4.3-2 illustrates an example of how the uplink traffic of various IP flows is transferred from the UE to UPF using QUIC multipath transport, and how the UPF relays this traffic to a final destination (remote host), although this solution does not preclude other forms of deployment in which the final destination may be associated with any IP address or a specific subnetwork.

Each IP flow is associated to a QUIC connection and to an associated bidirectional QUIC stream, which is configured to apply a specific steering mode for the uplink traffic. For example, the red IP flow is associated with the multipath QUIC connection #1 and with the red Stream Y, which is configured to apply the Smallest delay steering mode in the uplink direction.

All IP flows shown in this figure, except the blue IP flow, are transferred with the datagram transport mode (mode 1 or mode 2), i.e. their data packets are transferred inside QUIC DATAGRAM frames. The blue IP flow is transferred with the stream transport mode, so its data packets are transferred inside QUIC STREAM frames.

The downlink traffic of IP flows is transferred between the UE and UPF in a similar way.



Figure 6.2.4.3-2: Example of user-plane operation using the MPQUIC-IP steering functionality (UL direction)

### 6.2.5 Solution #2.5: MPQUIC steering functionality using Ethernet proxying over HTTP

#### 6.2.5.1 Introduction

The solution in this clause specifies a new ATSSS steering functionality, called Multipath QUIC-Ethernet (MPQUIC-E) steering functionality, and addresses the objective of KI#2.1 for a QUIC-based steering functionality to allow the transport of Ethernet frames over multiple access between UE and UPF.

This solution extends the MPQUIC functionality detailed in 3GPP TS 23.501 [3] Section 5.36.6.2.2 to enable steering, switching, and splitting of Ethernet traffic between the UE and UPF, in accordance with the ATSSS policy created by the network.

The solution is based on draft-ietf-masque-connect-ethernet [19] which specifies how Ethernet traffic can be transferred between a client (UE) and a proxy (UPF) using the HTTP/3 protocol [12]. The HTTP/3 protocol operates on top of the QUIC protocol [12], which supports simultaneous communication over multiple paths, as defined in draft-ietf-quic-multipath [19].

To allow negotiation of a tunnel for Ethernet over HTTP, draft-ietf-masque-connect-ethernet [8] defines the "connect-ethernet" HTTP upgrade token. The resulting Ethernet tunnels use the Capsule Protocol [12] with HTTP Datagrams. The HTTP datagram format includes a context ID (a 62-bit value) and a payload, with a semantic dependant on the value of the context ID field.

When associated with an Ethernet proxying stream the HTTP datagram payload field of HTTP datagrams, the value of the Context ID is set to zero (per [8]) and the Payload field contains a full Layer 2 Ethernet Frame (from the MAC destination field until the last byte of the Frame check sequence field). Ethernet proxying requests use HTTP Extended CONNECT. The requests use HTTP pseudo-header fields as described in Section 4.4 of [8].

Editor’s note: How this solution interacts with other "connect-x" based solutions to completely fulfil the scope of the KI #2.1 is FFS.

#### 6.2.5.2 High-level Description

The key principles of the solution are summarized below.

- After the Ethernet MA PDU Session establishment, the UE creates one or more multipath QUIC connections with the UPF. Each multipath QUIC connection is associated with a QoS flow, i.e. it carries the traffic mapped to a QoS flow.

- The UE operates as a connect-ethernet client and the UPF operates as a connect-ethernet proxy, both defined in draft-ietf-masque-connect-ethernet [8]. Therefore, the UE supports an HTTP/3 client and the UPF supports an HTTP/3 proxy, both of them operating over QUIC.

- On each of the established QUIC connections, the UE sends an extended HTTP CONNECT request to UPF (as defined in [8]) indicating that Ethernet proxying over HTTP is needed.

- When the UE wants to transmit an uplink packet of an Ethernet flow, the UE:

- Selects which QUIC connection will be used for the uplink traffic of the IP flow based on the QoS flow associated with the Ethernet flow;

- Creates a new bidirectional QUIC stream on the selected QUIC connection;

- Configures the QUIC stream to apply a steering mode (i.e. the steering mode that should be used for the uplink traffic of the IP flow based on the ATSSS rules); and

- Forwards to UPF the uplink packets of the Ethernet flow using multipath QUIC transport.

- When the UPF wants to transmit a downlink packet of an Ethernet flow, the UPF:

- Selects which QUIC connection will be used for the downlink traffic of the Ethernet flow (this QUIC connection is the same as the one selected by UE for the IP flow, assuming the QoS flow in UL and DL directions is the same);

- Selects a bidirectional QUIC stream on the selected QUIC connection (this QUIC stream is the same as the one created by the UE for the IP flow);

- Configures the QUIC stream to apply a steering mode (i.e. the steering mode that should be used for the downlink traffic of the IP flow based on the N4 rules); and

- Forwards to UE the downlink packets of the IP flow using multipath QUIC transport.

The following figure illustrates how the traffic of an Ethernet flow is transferred between the UE and UPF using multipath QUIC transport [19]. In this figure, it is assumed that the uplink traffic and the downlink traffic of the Ethernet flow are mapped to the same QoS flow (QFI-1). Therefore, both the uplink traffic and the downlink traffic of the IP flow use the same multipath QUIC connection.



Figure 6.2.5.2-1: Using multipath QUIC transport for an Ethernet flow

The bidirectional QUIC stream is established by the UE to enable transmission of uplink Ethernet packets (blue) and downlink Ethernet packets (red) of the Ethernet flow. The UE configures this stream to send uplink traffic with a steering mode determined based on the ATSSS rules in the UE (uplink steering mode). The UPF configures this stream to send downlink traffic with a steering mode determined based on the N4 rules in the UPF (downlink steering mode). The data packets of the Ethernet flow shown in Fig. 6.12.2-1 are transmitted in datagram mode (mode 1 or mode 2), i.e. they are encapsulated in HTTP datagrams and QUIC DATAGRAM frames, each one carrying header information (see the Quarter Stream ID defined in RFC 9114 [9]) that associates it with the established bidirectional stream. As discussed below, the Ethernet frames packets of the Ethernet flow may be transmitted in stream mode (instead of datagram mode), i.e. transmitted directly over the bidirectional stream. In this case, the Ethernet packets of the Ethernet flow are encapsulated in DATAGRAM capsules and QUIC STREAM frames.

Figure 6.2.5.2-2 and Figure 6.2.5.2-3 illustrate the components of the MPQUIC-E steering functionality used to support data transmission in the uplink and downlink direction respectively. The MPQUIC-E steering functionality is composed of three components:

1) QoS flow selection & Steering mode selection: This component in the UE initiates the establishment of one or more QUIC connections, after the establishment of the MA PDU Session and, for each uplink IP flow, it selects a QoS flow (based on the QoS rules), a steering mode (based on the ATSSS rules) and a transport mode (see further details below). This component in the UPF selects, for each downlink Ethernet flow, a QoS flow (based on the N4 rules), a steering mode (based on the N4 rules) and a transport mode (see further details below)

In the UE, this component is only used in the uplink direction, while, in the UPF, this component is only used in the downlink direction.

2) HTTP/3 layer: Supports the HTTP/3 protocol defined in RFC 9114 [9] and the extensions defined in:

- draft-ietf-masque-connect-ethernet [8] for supporting Ethernet proxying over HTTP; and

- RFC 9297 [11] for supporting HTTP datagrams.

The HTTP/3 layer selects a QUIC connection to be used for each Ethernet flow and allocates a new QUIC stream on this connection that is associated with the Ethernet flow. It also configures this QUIC stream to apply a specific steering mode (further details are provided below).

In the UE, the HTTP/3 layer implements an HTTP/3 client, while, in the UPF, it implements an HTTP/3 proxy.

3) QUIC layer: Supports the QUIC protocol as defined in the applicable IETF specifications (RFC 9000 [12], RFC 9369 [18],RFC 9001 [13] and the extensions defined in:

- RFC 9221 [15] for supporting unreliable datagram transport with QUIC; and

- draft-ietf-quic-multipath [16] for supporting QUIC connections using multiple paths simultaneously.



Figure 6.2.5.2-2: Components of MPQUIC-E steering functionality used for UL data transmission



Figure 6.2.5.2-3: Components of MPQUIC-E steering functionality used for DL data transmission

The protocol stack of the solution is depicted in Figure 6.2.5.2-4 below.



Figure 6.2.5.2-4: UP protocol stack of the solution

#### 6.2.5.3 Procedures

Figure 6.2.5.3-1 below depicts the key steps of the procedure that enables data traffic to be exchanged between the UE and UPF using the MPQUIC-E steering functionality.



Figure 6.2.5.3-1: Procedure for enabling data traffic using the MPQUIC-E steering functionality

1. The UE establishes an Ethernet MA PDU Session with the 5G core (5GC) network. During the MA PDU Session establishment:

- In the PDU Establishment Request message, the UE indicates that it supports the MPQUIC-E steering functionality. This indication can be used by the network (a) to select a UPF that also supports the MPQUIC-E steering functionality and (b) to decide whether the ATSSS/N4 rules for the MA PDU Session may use the MPQUIC-E steering functionality.

- The UE receives MPQUIC-E proxy information, i.e. one IP address of UPF, one UDP port number and the proxy type (e.g. "connect-ethernet"). This information is used by the UE for establishing QUIC connections with the UPF, which is also referred to as "MPQUIC-E proxy".

- The UE receives one Ethernet MAC address for the Ethernet MA PDU Session and two additional IP addresses/prefixes, called "link-specific multipath QUIC" addresses; one associated with 3GPP access and another associated with the non-3GPP access. These two addresses can be used by the UE to create two paths in a multipath QUIC connection.

- The UE receives QoS rules and ATSSS rules to be applied for the MA PDU Session, for QoS enforcement and traffic steering enforcement respectively. Similar rules (N4 rules) are received by UPF.

2. After the MA PDU Session is established and the UE identifies that one or more ATSSS rules require traffic steering using the MPQUIC-E steering functionality, the UE determines the number of multipath QUIC connections to be established with the UPF (MPQUIC-E proxy). For example, the UE may determine to establish 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. The QoS rules provided to UE include downlink QoS information and the UE applies the downlink QoS information to establish QUIC connections for the QoS flows used for downlink traffic only.

3. The UE establishes the number of multipath QUIC connection with the UPF (MPQUIC-E proxy) determined in the previous step. This results into several multipath QUIC connections between the UE and UPF, each one composed of multiple paths, e.g. one path over 3GPP access and another path over non-3GPP access. Data transmitted over a multipath QUIC connection must be encrypted according to RFC 9001 [13].

During a QUIC connection establishment, the UE and UPF negotiate QUIC transport parameters and indicate (a) support of QUIC Datagram frames and (b) support of multipath. They indicate support of QUIC Datagram frames by providing the "max\_datagram\_frame\_size" transport parameter with a non-zero value (see RFC 9221 [9]) and they indicate support of multipath by providing the "enable\_multipath" transport parameter (see draft-ietf-quic-multipath [16]).

After a QUIC connection establishment, the HTTP/3 client and the HTTP/3 proxy negotiate HTTP settings and indicate support of HTTP Datagrams (see RFC 9297 [11]) and support of Extended CONNECT (see RFC 9220 [19]).

The QoS flow associated with a QUIC connection is also negotiated between the UE and UPF. This is done by using a new QUIC transport parameter (defined by 3GPP) when the QUIC connection is established.

NOTE 1: QUIC transport parameter needs to be registered in IANA (by stage 3).

4. On each of the established QUIC connections, the UE sends an extended HTTP CONNECT request to UPF (as defined in draft-ietf-masque-connect-ethernet [8]) indicating that Ethernet proxying over HTTP is needed. If this is accepted by UPF, it responds with a 200 status.

5. The UE generates a new Ethernet packet (Ethernet packet #1) that should be sent via the MA PDU Session. This packet initiates a new Ethernet flow, i.e. a sequence of Ethernet packets using the same source and destination and protocol field. For this new Ethernet flow (and for each new ones):

- The UE selects a QoS flow (QFI) over which the Ethernet flow should be transmitted. This is selected by using the received QoS rules.

- The UE selects a steering mode that should be applied for the flow. This is selected by using the received ATSSS rules.

- The UE selects a transport mode, e.g. a datagram transport mode or the stream transport mode. This is selected by using the received ATSSS rules, i.e. each ATSSS rule which indicates that the MPQUIC-E steering functionality should be applied for the matching traffic, indicates also the transport mode that should be applied for this traffic.

The datagram transport modes that are supported are the one described in Section 5.32.6.2.2.1 of [3].

6. The UE selects a multipath QUIC connection to be used for the new Ethernet flow (e.g. based on the selected QFI) and the UE allocates a new QUIC stream (e.g. stream 40) in this multipath QUIC connection. This new stream is associated with the new Ethernet flow. The UE configures the new stream to transmit data traffic using the selected steering mode for this flow.

7. The UE sends the Ethernet packet using the allocated new stream on the selected QUIC connection.

8. When an Ethernet packet is received by UPF (MPQUIC-E proxy) from the remote host (Ethernet packet #2), this packet is transferred to the UE using the established context information for the Ethernet flow, i.e. using the selected multipath QUIC connection, the selected stream on this connection, the selected steering mode, and the selected transport mode. Such context information is stored in the UPF and in the UE and is applied for all the Ethernet packets of the flow.

9. Similarly, when another packet is generated by the UE app (Ethernet packet #3), this packet is transferred to UPF (MPQUIC-E proxy) using again all the stored context information for that flow.

NOTE 2: The context information for an Ethernet flow in the UE and in the UPF is created when the initial Ethernet packet (i.e. Ethernet packet #1) of this flow is transferred. All subsequent packets of the same flow are transferred between the UE and the UPF using this context information.

When the UE identifies that the context information for an Ethernet flow is no longer needed, the UE deletes this context information and releases the associated QUIC stream, which cause the UPF to delete the context information stored in UPF.

The following figure 6.2.5.3-2 illustrates an example of how the uplink traffic of various Ethernet flows is transferred from the UE to UPF using QUIC multipath transport, and how the UPF relays this traffic to a final destination (remote host). Note that, for each flow there is an associated QUIC connection and an associated bidirectional QUIC stream, which is configured to apply a specific steering mode for the uplink traffic. For example, the red flow is associated with the multipath QUIC connection #1 and with the red Stream Y, which is configured to apply the Smallest delay steering mode in the uplink direction.

All flows shown in this figure, except the blue flow, are transferred with the datagram transport mode (mode 1 or mode 2), i.e. their data packets are transferred inside QUIC DATAGRAM frames. The blue Ethernet flow is transferred with the stream transport mode, so its data packets are transferred inside QUIC STREAM frames.

The downlink traffic of Ethernet flows is transferred between the UE and UPF in a similar way.



Figure 6.2.5.3-2: Example of user-plane operation using the MPQUIC-E steering functionality (UL direction)

### 6.2.6 Solution #2.6: for KI#2.2

#### 6.2.6.0 Introduction

As shown in the following figure, the UE accesses via both 3GPP and non-3GPP (WLAN) accesses to the network. On the 3GPP side, the UE transfers the NAS message to the AMF, and receives the UPF IP Address for non-3GPP access in the PDU Session establishment accept message. On the non-3GPP sides, the UE connects to the UPF indicated by the UPF IP address received from PDU Session establishment accept message. In order to establish the security connection via non-3GPP access, the UE shall use the IKEv2 messages in order to establish the IPSec security association.

In this architecture, the UPF is enhanced to support a new functionality with a public UPF IP addressfor the IPSec tunnel to be established between the UPF and the UE. The procedure to establish the IPSec tunnel is similar as the procedure defined for the UE and the ePDG.

In this solution, the UE only registers to the 3GPP side, and there is no registration via non-3GPP. If the UE is deregistered from 3GPP side or if the PDU session is released via 3GPP access, all the related CN resource including the IPSec tunnel if existing in the UPF shall be released.

Editor’s note: When the deactivation of UP connection over 3GPP side occurs, whether to release the IPSec tunnel over non-3GPP is FFS.



Figure 6.2.6-1: ATSSS-Lite solution #2.6 architecture

#### 6.2.6.1 PDU Session establishment of Solution #2.6



Figure 6.2.6.1: PDU Session establishment of Solution #2.6

3GPP Access:

Step 1: UE sends MA PDU Session establishment request to AMF based on the current specification.

Editor’s note: Whether to reuse "MA PDU session indication" or to define a new indication is FFS.

Editor’s note: Whether to define a new ATSSS-Lite capability in the UE’s ATSSS Capabilities is FFS.

Step 2: AMF sends the CreateSMContext Message to SMF.

Step 3: SMF retrieves the SM subscription data of the UE from UDM.

Step 4: If dynamic PCC is to be used for the MA PDU Session, the SMF sends an "MA PDU Request" indication and ATSSS Capabilities to the PCF in the SM Policy Control Create message PDU Session. The PCF provides PCC rules that include MA PDU Session Control information, as specified in TS 23.503 [5].

Editor’s note: Whether there is some impact on the use of MA PDU Session Control information is FFS.

Step 5: SMF selects the UPF, and initiates the N4 Session Establishment procedure with the selected UPF.

Step 6: The SMF requests the UPF to activate the IPSec functionality of the UPF, apart from the existing operation, e.g. to activate the MPTCP functionality/MPQUIC functionality as defined in TS 23.502 [4]. Based on the SMF request, the UPF allocates the IP address for the IPSec functionality of the UPF.

Step 7: The UPF 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.

As an alternative to step 6&7, the SMF sends to the UPF with the PDU Session ID and GPSI, and the UPF allocates IP address for the IPSec functionality of the UPF related to the PDU Session ID and GPSI.

Step 8: SMF sends N1N2 message to AMF including the PDU Session Establishment Accept message. In this PDU Session Establishment Accept message, the SMF includes the ATSSS rules for the MA PDU Session, and may include Measurement Assistance Information and/or the "MPTCP link-specific multipath" and/or "MPQUIC link-specific multipath" addresses/prefixes of the UE if the ATSSS-LL functionality or/and MPTCP functionality or/and MPQUIC functionality is to be applied. Additionally, the SMF also includes the UPF IP address received in step 7 from UPF in the PDU Session Establishment Accept message.

Step 9 - 10: AMF transfers the PDU Session Establishment Accept message to the UE via RAN. The UE receives the UPF IP address from SMF.

Till now, the UE established the MA PDU Session but with only one leg via 3GPP access.

Non-3GPP Access:

Step 1: Data Link Layer L2 is connected. The UE obtains the UE IP address from WLAN access network for the IPSec Tunnel Establishment with the UPF.

Step 2: 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.

Step 3: UE sends the IKE\_AUTH\_request to UPF with the UE NAI and the UE IP address received from the PDU Session Establishment Accept message via 3GPP access.

Alternatively, the UE requests connectivity to the PDU Session providing the PDU Session ID and GPSI, that are conveyed with IKEv2 (e.g., in the IDr payload).

Step 4: UPF determines the related N4 Session based on the UE IP address, then sends the UE NAI to the SMF via the related N4 Session. If the UPF cannot find the N4 Session according to the UE IP address, the UPF shall reject the UE request.

Step 5: Based on the received UE NAI, the SMF triggers the authentication procedure. The SMF constructs an EAP Response/Identity message that contains the UE NAI and sends the EAP Response/Identity message within Nausf\_SMauthentication\_Authenticate Request message to the AUSF.

Step 6: The AUSF selects a UDM as described in clause 6.3.8 of TS 23.501 [3] and obtains the authentication data from UDM for this UE.

Step 7-9: Based on the UE authentication data, the AUSF creates the EAP-Request/AKA'-Challenge message to the SMF in a Nausf\_SMAuthentication\_Authenticate Response message. The SMF shall transparently forward the EAP-Request/AKA'-Challenge message to the UPF via the related PFCF session. Then the UPF sends the EAP-Request/AKA'-Challenge message to the UE via IKE\_AUTH Answer message. The IKEv2 messages exchanged between the UE and the UPF are the same as the IKEv2 messages exchanged between the UE and the ePDG as defined in TS 33.402 [20] subclause 8.2.2.

Step 10: The AUSF and the UE may exchange EAP-Request/Response messages via the SMF and UPF. The SMF and UPF shall transparently forward these messages.

Step 11-12: After the UE is successfully authenticated, the AUSF shall send an EAP-Success message and security key to the SMF inside Nausf\_SMAuthentication\_Authenticate Response message. The SMF forwards the EAP-Success message and the key to the UPF via N4 Session.

Step 13-14: The UPF sends EAP-Success message to the UE, and completes the IPSec Tunnel establishment procedure based on the Key received from the SMF.

The UE establishes the MA PDU Session with two legs on both 3GPP and non 3GPP access, and performs the traffic steering, switching and splitting based on the ATSSS rules following the current mechanism. The UE sends the uplink data encapsulated in the IPSec tunnel with the inner source IP address set to the UE IP address or "MPTCP link-specific multipath" addresses/prefixes of the UE or "MPQUIC link-specific multipath" addresses/prefixes of the UE based on the steering functionality to be applied.

Editor’s note: It is FFS how to correlate the traffic over 3GPP access and non 3GPP access in the UPF for the MA PDU Session, e.g. by using the N3 tunnel info over 3GPP access and the SPI associated with the IPsec over non 3GPP access.

Editor’s note: Whether there is any security risk to expose the public IP address of the UPF to the UE is to be investigated by SA3.

#### 6.2.6.2 System impact

The solution has impact on the UE and some NFs, as follows.

UPF:

* Supports the ATSSS-Lite functionality, including allocation of the public IP address for this ATSSS-Lite functionality, establishment of the IPSec tunnel with the UE, and forwarding the UE NAI and EAP messages to the SMF via the N4 Session.

SMF:

* Supports a new interface with AUSF for exchanging the new Nausf\_SMAuthentication\_Authenticate Request/Response messages. In addition, the N4 interface needs to be enhanced to transport the UE NAI, EAP messages and security Key.

AUSF:

* Supports a new interface with SMF for exchanging the new Nausf\_SMAuthentication\_Authenticate Request/Response messages.

UE:

* Supports to transfer the UPF IP address for non-3GPP access in the NAS message over 3GPP access, and supports to establish IPSec tunnel with the UPF for transport of traffic over non-3GPP access.

Editor’s note: Other system impact is FFS.

### 6.2.7 Solution #2.7: Architecture for ATSSS-Lite

#### 6.2.7.1 Description

##### 6.2.7.1.1 Introduction

This solution addresses KI 2.2 (Simplified ATSSS architecture over non-3GPP access) and introduces the architecture for a lightweight version of ATSSS, name ATSSS-Lite. This new architecture is based on the principles described in the following subclauses. The solution does not apply to ATSSS-LL.

##### 6.2.7.1.2 Architecture without TNGF/N3IWF

This solution proposes an architecture in which there is no gateway for access to 5G CN via non-3GPP access, such as TNGF (for trusted non-3GPP access) or N3IWF (for untrusted non-3GPP access). In particular, the UE does not establish any IPSec connection to the 5G CN. Instead, the UE connects to the UPF via the public IP network (Internet) over a new interface named Nx. The existing UPF and ATSSS related traffic handling is extended in such way that a PDU session over the NIN3Aused in ATSSS is logically replaced by a secure connection that is used to transfer UP traffic between UE and UPF. The connection between the UE and the UPF over the Nx interface is secured using TLS. There are no explicit resources reserved in the NIN3A, which just provides IP connectivity to the UE, allowing the UE to connect to the UPF in a secure manner. Traffic handling is done like in ATSSS, but with only difference that the non-3GPP access leg of the MA PDU Session is now replaced with the secure connection over NIN3A.

The **ATSSS-Lite** architecture, in case of non-roaming and roaming scenario is described in Figures 6.2.7.1.2-1 and 6.2.7.1.2-2, respectively.



Figure 6.2.7.1.2-1: Baseline ATSSS-Lite architecture (non-roaming scenario)



Figure 6.2.7.1.2-2: Baseline ATSSS-Lite architecture (roaming scenario)

It is assumed that the UPF acting as anchor for the ATSSS-Lite connectivity supports the new Nx interface. The UPF processes the traffic according to the traffic handling rules (MAR/N4 rules) provided by the SMF (this aspect is inherited from ATSSS and is described more in detail in subclause 6.2.7.1.4).

Editor’s Note: security aspects related to exposing a new IP communication endpoint to be reachable directly by the UE over non-3GPP access may need further investigation by SA3.

##### 6.2.7.1.3 Non-Integrated Non-3GPP Access and re-use of the MA PDU Session concept

The ATSSS-Lite architecture leads to the notion of **Non-Integrated Non-3GPP Access (NIN3A)** (see clauses 3.1 and 3.2). The solution proposes to reuse the definition of **Multiple Access PDU Session** described in TS 23.501 [3] clause 3.1 **for NIN3A**, which reads as follows:

***MA PDU Session:*** *A PDU Session that provides a PDU connectivity service, which can use one access network at a time, or simultaneously one 3GPP access network and one non-3GPP access network.*

Figure 6.2.7.1.3-1 depicts a simplified diagram of a MA PDU Session applied to one 3GPP access and one Non-Integrated Non-3GPP Access.



Figure 6.2.7.1.3-1: MA PDU Session with Non-Integrated Non-3GPP Access

##### 6.2.7.1.4 Re-use of high layer steering functionality and traffic security

The assumption for ATSSS-Lite is that the steering functionalities in the UE and in the UPF are high layer steering functionalities. They are based on the existing MPTCP and MQUIC steering functionalities that are used in the legacy ATSSS (see TS 23.501 [3] clauses 5.32.6.2.1 and 5.32.6.2.2).

Editor's Note: Whether only the MPQUIC functionality or both the MPQUIC and the MPTCP steering functionalities are going to be supported, can be decided based on the conclusion of KI#2.1 (MPQUIC steering functionality to steer, switch and split non-UDP traffic).

The traffic exchanged between UE and UPF (in terms of confidentiality and integrity protection) can be protected using the Transport Layer Security protocol (TLS).

NOTE: Further security details can be discussed by SA3, if and when needed.

##### 6.2.7.1.5 Protocol stacks connectivity via Non-3GPP

The solution is based on the following assumptions:

* The NAS signaling between UE and CN is carried only over the 3GPP access. This implies that there is no need to have NAS signaling between UE and CN exchanged over NIN3A when the UE is connected via 3GPPA. Consequently, no CP protocol stack between UE and CN over Nx interface is needed.

Editor's Note: Whether and how there is a need to establish, manage and maintain communication between UE and UPF via NIN3A when the UE is not connected via 3GPPA is FFS.

- Since, as explained in 6.2.7.1.4, there is no need for establishment of an IPSec tunnel between UE and network over NIN3A, the UE UP protocol stack for the non-3GPP access can be simplified. Figure 6.2.7.1.5-1 depicts the user plane protocol stack over Nx interface. The solution does not use primary (AKA based) authentication via non-3GPP access and relies on that the UE has been authenticated via 3GPP access.

Editor’s Note: Security aspects, including aspects related to the exposure of a new IP communication endpoint to be reachable directly by the UE over non-3GPP access, are assumed to be further investigated by SA3.



Figure 6.2.7.1.5-1: UP Protocol Stack for Nx interface

##### 6.2.7.1.6 Re-use of steering modes, MPTCP/MQUIC measurements and extension URSP/ATSSS/N4 rules

Since the steering functionality for ATSSS-Lite is based on MPTCP or MPQUIC, the MPTCP/MQUIC measurements mechanisms can be used instead of the 3GPP defined PMF (Performance Measurement Function) to measure Round Trip Time (RTT) and Packet Loss Rate (PLR). Because of that, at least in principle, the existing ATSSS steering modes (with thresholds, where applicable), namely, Load Balancing, Shortest Delay, Active-Standby, Priority Based and Redundant Steering Mode can be applied also to MA PDU Sessions with NIN3A.

Similarly, the URSP rules, currently used in the 5GS by the PCF to indicate to the UE which traffic is subject to ATSSS, can be extended to indicate which traffic is subject to ATSSS-Lite (i.e., which traffic can be transferred using NIN3A). The same principle can be applied to the ATSSS rules (for the UE) and the MAR/N4 rules (for the UPF), so that the SMF can indicate to the UE and UPF *how* the traffic subject to ATSSS-Lite is to be handled.

Editor’s Note: Details of how URSP rules, ATSSS and MAR/N4 rules can be extended are FFS.

#### 6.2.7.2 Procedures

The procedures in this clause describe how the MA PDU Session can be established for ATSSS-Lite and how the appropriate SMF and UPF can be selected according to the indicated UE capability. Figures 6.2.7.2.1-1 and 6.2.7.2.1-2 describe two options of how a MA PDU Session over the Nx interface can be established. Such Figures are based on a simplified version of TS 23.502 [4] Figure 4.3.2.2.1-1 and on the procedure described in TS 23.502 [4] clause 4.22.2.1, with the key enhancements highlighted.

In the procedures, SMF selects the UPF based on an ATSSS-Lite indication from the UE, and then the SMF requests the UPF for its Access Info data to be used with this MA PDU session. Access Info data includes communication parameters of how the UPF may be reached, such as IP addresses, port numbers or FQDNs, credentials, security keys and other relevant information depending on the used steering functionality, i.e., MP-QUIC. One Access Info data may be associated with one MA PDU session, and it is steering functionality specific. In addition, the Access Info data is dynamic in nature, and it may have lifetime during which the UPF is reachable for the UE to establish a secure connection via the NIN3A. If the UE has not managed to establish a secure connection within the given timeframe, then the given Access Info data is expired, and the UE needs a new one by requesting PDU Session modification from the SMF (as shown in Figure 6.2.7.3‑2). It is the UPF's responsibility to provision and monitor this lifetime.

##### 6.2.7.2.1 Option 1: ATSSS capable AMF

This option assumes that the AMF supports ATSSS-Lite.



Figure 6.2.7.2.1-1: Simplified ATSSS-Lite MA PDU Session Establishment – Option 1

The main steps of the MA PDU Session Establishment procedure for ATSSS-Lite can be summarized as follows:

1. When sending the PDU Session Establishment Request to the CN, the UE Includes a request to establish a MA PDU Session Request as well as its ATSSS-Lite capability indication.

2. Based on such indication and request, the AMF selects an ATSSS-Lite capable SMF (which may, but does not have to, support legacy ATSSS), or if no such SMF is available, rejects the request and notifies the UE.

3. The AMF forward the indications from the UE to the SMF.

4. The SMF, based on the ATSSS-Lite capability indication of the UE forwarded by the AMF and with the help of NRF, selects a UPF that is configured to receive/send traffic over the Nx interface. If no such UPF is available, the session cannot be established, and this is notified to the UE.

5. The SMF establishes SM policy association with the PCF and receives ATSSS rules. The SMF establishes the UP resources in the UPF and instructs it with the related N4 Rules. The SMF instructs the UPF to activate MPTCP or MPQUIC functionality, and requests Access Info data from the UPF and the UPF sets new timer for the Access Info data. The UPF allocates the UE "MPTCP link-specific multipath" or the UE "MPQUIC link-specific multipath" addresses/prefixes.

6. The SMF establishes the necessary UP resources over the 3GPP access network, indicates the ATSSS rules to the UE. The SMF provides to the UE the Access Info data, including the MPTCP or MPQUIC link-specific multipath addresses/prefixes of the UE and the MPTCP or MPQUIC proxy and the necessary information (e.g., TLS security material including any required certificates for MPTCP/MPQUIC Proxy) for the UE to establish the MPTCP/MQUIC session over NIN3A.

After step 6, the UE is able to establish the communication with the UPF via NIN3A/Nx interface. For MP-QUIC, once the PDU Session is established the UE first establishes an MP-QUIC connection with the UPF and adds the first path of the MP-QUIC connection via the 3GPP access. If the UE also has another IP connectivity via a NIN3A, the UE then creates a second MP-QUIC path to the UPF over the NIN3A using the Access Info data received from the SMF during PDU Session establishment. The QUIC layer takes care of using the existing secure context that was created when the MP-QUIC connection was established over 3GPP access.

As soon as the communication is established, the UE and the UPF can exchange UP data over both accesses according to the ATSSS rules and the MAR/N4 rules received from the SMF.

##### 6.2.7.2.2 Option 2: ATSSS capable SMF supports ATSSS-Lite

This option assumes that an ATSSS capable SMF supports ATSSS-Lite, whereas the AMF is transparent to ATSSS-Lite.



Figure 6.2.7.2.2-2: Simplified ATSSS-Lite MA PDU Session Establishment – Option 2

With the assumptions above, Option 2 is based on the same steps of Option 1, with the key difference that the (legacy) ATSSS capability indication is sent by the UE to enable the AMF to select the SMF, while the SMF selects an ATSSS-Lite capable UPF (i.e., a UPF capable to receive/transmit traffic over the Nx interface) based on the ATSSS-Lite capability indication included in the extended protocol configuration option IE (ePCO) of the PDU Session Establishment message.

##### 6.2.7.2.3 Enhancements to MA PDU Session Modification



Figure 6.2.7.2.3-1: MA PDU session modification for using NIN3A

Step 1: The UE issues new PDU session modification request (for the MA PDU session supporting ATSSS between 3GPP and NIN3A) to get a new Access Info data.

Step 2: The SMF requests Access Info data from the PSA UPF of MA PDU Session.

Step 3: The SMF provides Access Info data in Session Modification Accept to the UE.

Step 4: Using Access Info data, the UE adds a new path (e.g. to the MP-QUIC connection, QUIC takes care of security etc.).

NOTE: While Access Info data is valid, the UE may try to repeat Step 4, via different NIN3A.

#### 6.2.7.3 Impacts on services, entities and interfaces

UE:

- Indicates UE ATSSS-Lite Capability.

Editor’s Note: whether this is indicated only in SM signalling at PDU session establishment or also to AMF is FFS.

- Receives Access Info data from the SMF.

- Creates new MPTCP/MP-QUIC path to the existing MA PDU session using the received Access Info data.

- Ability to request new Access Info data from the SMF via PDU Session modification procedure.

AMF (in option 1 only):

- Uses UE ATSSS-Lite Capability to select ATSSS-Lite capable SMF.

SMF:

- Uses UE ATSSS-Lite Capability provided by the UE to select ATSSS-Lite capable UPF

- Provisioning of new MPTCP/MPQUIC information between UPF and UE.

- Support of MA PDU Sessions via non-3GPP access without a SM NAS connection via non-3GPP access. This includes handling of the MA PDU Session in case the UE is not reachable via 3GPP access.

- Indicates to UE whether ATSSS-Lite MA PDU Session is accepted or not.

- Receives in PDU Session establishment request, an indication for support of ATSSS-Lite and selects an UPF that supports this feature.

- Query Access Info data from the UPF and provide it to the UE.

- Receives request from UE, in PDU Session Modification, to fetch fresh Access Info data from UPF, Query Access Info data from the UPF and provide it to the UE.

UPF:

- Supports Nx interface by exposing new communication endpoint(s) (i.e., Access Info data) reachable via NIN3A network for adding a new path for the MPTCP/MP-QUIC connection.

- Provides Access Info data when requested by SMF.

- Provisions and monitors of Access Info data lifetime.

### 6.2.8 Solution #2.8: Simplified ATSSS over non-3GPP based on direct MPQUIC connection between UE and UPF

#### 6.2.8.1 Description

##### 6.2.8.1.1 General

This solution addresses KI#2.2.

Since QUIC is encrypted, there is a possibility to use the MPQUIC Steering Functionality between UE and UPF without the underlying IPSec layer and without a Gateway such as N3WIF or TNGF (subject to SA3 analysis and confirmation). In this case there is no NAS signalling connection via non-3GPP access, and therefore the MA PDU Session needs to be established and managed via 3GPP access.

This solution is based on the following basic principles and assumptions:

- N3IWF/TNGF is not used when accessing over non-3GPP access.

- The NAS procedures over 3GPP access are used to register in 5GC and establish MA PDU Session.

- The NAS procedures via 3GPP access are also used to provision the UE with necessary information to connect towards the UPF with MPQUIC over non-3GPP access.

- UE has no N1 (NAS) signalling connection with the 5G Core (5GC) network over non-3GPP access.

- In order to add non-3GPP access user plane resources for a MA PDU Session, the UE first has to establish a PDU Session with 5GC over 3GPP access.

- The UPF (PSA) has at least one transport address (i.e. an IP address and a port number) that is reachable via the Internet.

- The solution only supports MPQUIC Steering Functionality. ATSSS\_LL and MPTCP are not supported.



Figure 6.2.8.1.1-1: Architecture for simplified ATSSS over non-3GPP based on direct MPQUIC connection between UE and UPF

The Nx reference point supports MPQUIC connectivity between UE and UPF and is based on existing MPQUIC interface between UE and UPF.

The solution does not use primary (AKA based) authentication via non-3GPP access and relies on that the UE has been authenticated via 3GPP access.

Editor’s Note: Security aspects, including aspects related to the exposure of a new IP communication endpoint to be reachable directly by the UE over non-3GPP access, are assumed to be further investigated by SA3.

#### 6.2.8.2 Procedures

##### 6.2.8.2.1 General

The procedures below describe two options:

- Option 1: In this option, the MA PDU session establishment procedure is transparent to the AMF.

- Option 2: In this option the AMF is enhanced to support simplified ATSSS procedures over non-3GPP access.

##### 6.2.8.2.2 Registration via 3GPP access

Option 1 (MA PDU session establishment procedure is transparent to the AMF):

- In this option there are no impacts to the registration procedure via 3GPP access

Option 2 (AMF is enhanced to support simplified ATSSS procedures over non-3GPP access):

- During the Registration procedure the network indicates to the UE the ATSSS feature that it supports, i.e. the Registration Accept message may contain an indication that the network supports only the simplified ATSSS feature, or that it supports only the legacy ATSSS feature, or that it supports both the simplified and the legacy ATSSS.

##### 6.2.8.2.3 MA PDU Session Establishment via 3GPP access



Figure 6.2.8.2.3-1: PDU Session Establishment over 3GPP access

Option 1 (without AMF impacts):

1. The UE sends a PDU Session Establishment Request message and includes its ATSSS Capabilities, also indicating that it is capable of "direct ATSSS via non-3GPP access using MPQUIC".

NOTE 1: This option is assumed to be transparent to the AMF. The handling of the MA PDU Session from SMF point of view towards AMF is thus different compared to rel-18.

2. The AMF selects an SMF and sends a Nsmf\_PDUSession\_Create Request message with the PDU Session Establishment Request message. The SMF treats the PDU Session as an MA PDU Session that is capable of "direct ATSSS via non-3GPP access using MPQUIC".

Editor's note: How to handle SMF selection and the case where SMF does not support "direct ATSSS via non-3GPP access using MPQUIC" is FFS.

Option 2 (with AMF impacts):

1. The UE sends a PDU Session Establishment Request message and includes within the PDU session establishment Request message the ATSSS capabilities it supports (e.g. "direct ATSSS via non-3GPP access using MPQUIC"), in accordance with the ATSSS feature which is supported by the network and has been indicated to the UE during the registration procedure.

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.

Steps that are common to Option 1 and Option 2:

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 "direct ATSSS via non-3GPP access using MPQUIC". The SMF may discover the UPF capabilities via NRF or the N4 Association establishment.

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. In this case MPQUIC is indicated together with an indication for "direct ATSSS via non-3GPP access using MPQUIC".

If the message from SMF instructs the UPF to activate MPQUIC functionality with "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.

The UPF also allocates a UE "MPQUIC link-specific multipath" address/prefix for 3GPP access and provides this to SMF, as per rel-18. The UPF does not allocate a UE "MPQUIC link-specific multipath" address/prefix for non-3GPP access.

NOTE 2: The UE uses the local IP address allocated by the non-3GPP access to reach the MPQUIC proxy via non-3GPP access.

The SMF also provides N4 rules, e.g. MAR, to the UPF.

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

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

- MPQUIC Proxy address information (IP address and port number) for 3GPP access

- MPQUIC Proxy address information (IP address and port number) for non-3GPP access

- Link-Specific Multipath IP address for 3GPP Access, as defined in TS 23.501 [3], 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 [3], clause 5.32.6.

NOTE 3: As described in 6.2.8.2.2, the UE local IP address used in non-3GPP is used by the UE for proxying traffic flows over non-3GPP access.

MA PDU IP address/prefix (i.e. UE IP address used on N6 for the MA PDU Session) is allocated to the UE via mechanisms defined in TS 23.501 [3], clause 5.8.2.2.

The SMF may also include ATSSS rules.

9. The rest of the MA PDU Session procedure is executed, as described in TS 23.502 [4].

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 [3] and TS 23.502 [4]. These multipath QUIC connection are established via 3GPP access, allowing the UPF to associate the QUIC connection with the PDU Session / N3 tunnel.

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 [16]).

- 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.

##### 6.2.8.2.4 Addition of non-3GPP access user-plane resources

The use of MPQUIC over non-3GPP access is based on the MPQUIC steering functionality in Rel-18, with the clarifications and changes described in this clause.



Figure 6.2.8.2.4-1: Addition of non-3GPP access user-plane resources

After MA PDU Session Establishment via 3GPP access, and after the multipath QUIC connections are established via 3GPP access, the UE may add non-3GPP access user plane resources. This is done by adding MPQUIC paths to the existing QUIC connection in the same way as already defined Rel-18 but with the difference that the UE uses the local IP address assigned by the non-3GPP access as the UE IP address and the non-3GPP MPQUIC proxy address and port received from SMF during MA PDU Session Establishment, as illustrated in Figure 6.2.8.2.2-1.

1. UE has an established MPQUIC connection with the UPF over 3GPP access, as described in clause 6.2.8.2.1.

2. UE obtains a local IP address from the non-3GPP access. This IP address, combined with a UE-assigned port number, is to be used as UE’s transport address for the MPQUIC path established over non-3GPP access and via the Internet.

3. UE initiates validation of the new path with the UPF via non-3GPP access as defined in the QUIC specification (IETF RFC 9000 [12]) and the QUIC multi-path extensions (IETF draft-ietf-quic-multipath [16]).

The UE selects an unused Connection ID provided by the UPF for the new path and sends a packet containing a PATH\_CHALLENGE frame, initiating the path validation process. This action demonstrates the UE's intention to establish or migrate to a new path using the selected Connection ID. The UPF receives the PATH\_CHALLENGE and responds with a PATH\_RESPONSE frame, acknowledging the challenge and completing the path validation process. This exchange ensures the UE and UPF can securely communicate over the new path.

The UPF sends a PATH\_CHALLENGE frame to the UE for path validation as part of its response. The PATH\_CHALLENGE frame contains data that the UE shall echo back in a PATH\_RESPONSE frame, proving the bidirectional validity of the path. This step is crucial for establishing that the UE can receive and send packets on this new path, providing assurance against potential address spoofing and ensuring the integrity of the connection path.

4-5. Once the new path has been validated, the UPF informs the SMF of the establishment of the new path using the N4 Session Report procedure.

6. Having been informed of the establishment of the new path, the SMF may provide updated N4 rules to the UPF using the N4 Session Modification procedure and may also provide updated ATSSS rules to the UE.

7. The UE and UPF can start sending data packets via the new path. Packets belonging to the same QUIC connection can be routed via either of the two paths.

Apart from the IP address aspects described above, the MPQUIC functionality over non-3GPP access follows the description in TS 23.501 [3], clause 5.32.6.2.2, i.e. there is no impact to the use of MPQUIC or HTTP/3 protocols as such. In particular, to support steering, switching and splitting, for each uplink UDP flow, the UE selects a QoS flow (based on the QoS rules), a steering mode and a transport mode (based on the ATSSS rules) and execute the required HTTP/3 signalling to proxy the UDP flow, as described in TS 23.501 [3]. In the same way, UPF performs steering, switching, and splitting of each downlink UDP flow based on the MAR rules.

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.

##### 6.2.8.2.5 Handling of the MA PDU Session in case the UE loses 3GPP access coverage

###### 6.2.8.2.5.1 General

In case the UE loses 3GPP coverage and is no longer reachable via 3GPP access, it is not possible to execute NAS procedures between the UE and 5GC. In this case the UE and SMF may keep the MA PDU Session active over non-3GPP access with limited capabilities (no support for PDU Session Modification) during a limited time, e.g. in case the UE returns to 3GPP coverage. The time limit for how long the MA PDU Session can be active via non-3GPP access without the UE being available in 3GPP access is determined by SMF based on operator policies. When the time expires, the SMF releases the MA PDU Session and also notifies UPF, PCF etc. Also the UE may decide to release the MA PDU Session.

Editor’s note: Whether and how it is possible to keep the MA PDU Session via non-3GPP access even if the UE is deregistered from 3GPP access is FFS.

###### 6.2.8.2.5.2 PCF- or SMF-initiated PDU Session release when UE is not reachable via 3GPP access

If the UE is not reachable via 3GPP access and the SMF wants to release the MA PDU Session, the SMF releases the N4 Session and the UPF releases the QUIC connections towards the UE and other context for the N4 session. This is described in following procedure.



Figure 6.2.8.2.5-1: PCF- or SMF-initiated PDU Session release when UE is not reachable via 3GPP access

0. The SMF or PCF determines to release the MA PDU Session.

1. The SMF may send a Namf\_Communication\_N1N2MessageTransfer Request with a PDU Session Release Command to the UE via 3GPP access. If the UE is not reachable, the AMF will send a Namf\_N1N2TransferFailureNotification to the SMF.

2. The SMF initiates a N4 Session Release Request to UPF.

3. The UPF removes the associated context and releases the QUIC connection(s) towards the UE. The UE will not trigger establishment of new QUIC connections in non-3GPP access for this MA PDU Session (As described in clause 6.2.8.2.2, QUIC connections are assumed to be established via 3GPP access).

4. The UPF replies to SMF.

5. The SMF terminates the SM policy association, if needed.

6. The SMF deregisters the PDU Session from UDM.

The PDU Session status will be synced between UE and network the next time the Registration procedure is executed via 3GPP access, as per existing specifications.

###### 6.2.8.2.5.3 UE-initiated PDU Session release via non-3GPP access when UE is not registered via 3GPP access.

If the UE wants to release the MA PDU Session and the 5GC is not reachable via 3GPP access, the UE releases the QUIC connection. If the SMF has requested the UPF to report access availability and unavailability, the UPF notifies the SMF that non-3GPP access is unavailable when the last QUIC connection for a N4 session is removed.



Figure 6.2.8.2.5-2: UE-initiated PDU Session release via non-3GPP access when UE is not registered via 3GPP access

0. The UE determines to release the MA PDU Session but is not reachable via 3GPP access.

1. The UE releases the QUIC connections towards UPF.

2. The UPF reports to SMF that the non-3GPP access is not available.

If the SMF becomes aware that the UE is not reachable via 3GPP access (e.g. in case downlink data arrives and it is not possible to establish the user plane connection via 3GPP access), the SMF may decide to start a timer and then trigger PDU Session release as described in clause 6.2.8.2.4.

The PDU Session status will also be synced between UE and network the next time the Registration procedure is executed via 3GPP access, as per existing specifications.

###### 6.2.8.2.5.4 Establishment of a MA PDU Session via non-3GPP access if 3GPP access is not available

Editor’s note: Whether and how this solution can be enhanced to support establishment of a MA PDU Session via non-3GPP access is FFS.

#### 6.2.8.3 Impacts on services, entities and interfaces

UE:

- Support for ATSSS using MPQUIC towards UPF without N3IWF/TNGF, using separate MPQUIC proxy address for 3GPP and non-3GPP accesses.

- Receives two MPQUIC Proxy address information items (instead of one in Rel-18) from the SMF: one each to be used by the QUIC client for QUIC paths established via 3GPP access and non-3GPP access, respectively.

- Receives one Link-Specific Multipath IP address (instead of two in Rel-18) to be used by the QUIC client via 3GPP access.

SMF:

- Ability to select a UPF capable of "direct ATSSS over non-3GPP access using MPQUIC".

- Provisioning of new MPQUIC proxy information between UPF and UE (e.g. MPQUIC proxy address for Nx interface).

- Support of MA PDU Sessions via non-3GPP access without a SM NAS connection via non-3GPP access. This includes handling of the MA PDU Session in case the UE is not reachable via 3GPP access.

- Receives access availability/unavailability reports from UPF for non-3GPP access based on the existence of QUIC connections.

UPF:

- ATSSS with MPQUIC connectivity without GTP-U tunnel.

- New UPF capability for "direct ATSSS via non-3GPP using MPQUIC" in N4 signalling and UPF profile in NRF.

- Trigger access availability/unavailability reports to SMF for non-3GPP access based on the existence of QUIC connections.

No impacts to UDM, PCF.

For option 1 there is no impact to AMF.

For option 2, there is the following impacts to AMF:

- Support for new capability indications to/from UE and support for selecting SMF supporting simplified ATSSS over non-3GPP access.

# 7 Overall Evaluation

Editor's note: This clause will provide evaluation of different solutions.

## 7.1 Overall Evaluation for DualSteer

Editor's note: This clause will provide evaluation of different solutions for DualSteer.

## 7.2 Overall Evaluation for ATSSS\_Ph4

Editor's note: This clause will provide evaluation of different solutions for ATSSS\_Ph4.

# 8 Conclusions

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities.

## 8.1 Conclusions for DualSteer

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities for DualSteer.

## 8.2 Conclusions for ATSSS\_Ph4

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities for ATSSS\_Ph4.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-01 | SA2#160-AH-e | S2-2401316 | - | - | - | Proposed skeleton approved at SA2#160-AH-e | 0.0.0 |
| 2024-01 | SA2#160-AH-e | - | - | - | - | Documented approved p-CR at S2#160-AH-e, including S2-2401618, S2-2401619, S2-2401620, S2-2401621, S2-2401637, S2-2401638 | 0.1.0 |
| 2024-03 | SA2#161 | - | - | - | - | Documented approved p-CR at S2#161, including S2-2402520, S2-2403250, S2-2403256, S2-2403546, S2-2403671, S2-24036712, S2-2403673, S2-2403674, S2-2403676, S2-2403677, S2-2403831, S2-2403832 | 0.2.0 |