**3GPP TSG-WG SA2 Meeting #139E e-meeting *S2-200xxxx***

**Elbonia, August 19 – September 1, 2020 (revision of S2-200xxxx)**

**Source: Huawei, HiSilicon**

**Title: Update QUIC solution to solve ENs**

**Document for: Approval**

**Agenda Item: 8.6**

**Work Item / Release: ATSSS / Rel-17**

*Abstract: This contribution addresses the Editor’s Notes with solution 8.*

# 1. Introduction/Discussion

In this paper, it solves the Editor’s Notes added in QUIC solution #8. The main changes include the following aspects:

1. Clarify the difference between the transparent and non-transparent solution.
2. Analyse the SOCKS5 protocol when it is applied between the UE and UPF.
3. Propose solutions to support the NULL encrypted QUIC connection.
4. Add the impacts on services, entities, interfaces and IETF Protocols.

Corresponding Editor’s Notes are removed.

# 2. Text Proposal

It is proposed to capture the following changes in 3GPP TR 23.700.

\* \* \* \* First change \* \* \* \*

### 6.8.2 High-level Description

The QUIC functionality in the UE applies the QUIC protocol defined by IETF draft-ietf-quic-transport-27: "QUIC: A UDP-Based Multiplexed and Secure Transport". It may be implemented by the operating system or by the application layer. This QUIC functionality in the UE will communicate with the QUIC Proxy functionality in the UPF or QUIC functionality in the remote server. The solution details for each case are described as below.

**QUIC connection between the UE and the UPF:**

The following Figure 6.8.2.-1 shows the QUIC functionality in the UE model and its relationship with the other functionalities.



Figure 6.8.2-1: QUIC Functionality in the UE

As shown in the above Figure 6.8.2-1, the application data is encapsulated by the QUIC functionality and then transported to the ATSSS-LL functionality. The ATSSS-LL functionality decides on the path for transport of the QUIC packet based on the link performance measurement of PMF. But different from the R16 ATSSS solution, in which the ATSSS-LL could only split a SDF per traffic on both accesses, the ATSSS-LL functionality can split a traffic per packet on both accesses with combination of QUIC functionality, to take advantage of both access resource to raise bandwidth, since the QUIC functionality supports the packet reordering with the sequence number included in the QUIC header. Especially, compared with TCP, the QUIC ACK frame contains one or more ACK ranges. Each ACK range could identify acknowledged packets and also contain additional ranges of packets which are alternately not acknowledged (Gap). With such enhancement, the QUIC protocol can solve the packet disordering issue received from lower layer, e.g. ATSSS-LL.

The traffic steering, switching or splitting is performed by the ATSSS-LL functionality, so there is no need to allocate the link-specific IP address for the UE as MPTCP functionality. Therefore, only one UE IP address of the MA PDU session is applied.

The QUIC proxy functionality is enabled in the UPF, and it can be transparent QUIC proxy, or non-transparent QUIC proxy. For both transparent and non-transparent solutions, the UE needs to enable the QUIC stack in the data path based on the QUIC steering method indication from SMF. The difference is that for transparent QUIC proxy, the traffic packets transported in the QUIC connection are encapsulated with the remote Server IP address, while for non-transparent QUIC proxy, the traffic packets transported in the QUIC connection are encapsulated with the QUIC proxy IP address. The protocol stack for both transparent and non-transparent QUIC proxy is as described in Figure 6.8.2-2.

NOTE 1: In case TLS 1.3 is applied, the UE will accept the credential of UPF during QUIC connection establishment procedure for both transparent and non-transparent QUIC proxy, as the UE knows the QUIC connection is established between the UE and UPF.

NOTE 2: There is no need to support both transparent and non-transparent proxy.

- Transparent QUIC proxy solution: The UE and UPF establish the QUIC connection, and the UPF apply regular UDP to the remote host. The packet from the UE is encapsulated with the destination IP address of the remote server. The QUIC packet is received in the QUIC connection. The UPF removes the QUIC header and then forward it to the remote host by using UDP.

- Non-transparent QUIC proxy solution: similar with MPTCP solution in R16, the network shall send QUIC proxy information to the UE, i.e. the QUIC functionality IP address, a port number. The UE will use this QUIC IP address as the destination IP address to encapsulate the user data and the UPF updates it to the remote host IP address. The following IETF protocol is needed in this non-transparent QUIC solution, e.g. to transport the IP address of the remote server to the UPF:

- Socks v5: IETF RFC 1928 [11]. "SOCKS Protocol Version 5".

The call flow is defined as below based on the IETF RFC 1928 [11].



Figure 6.8.2-2: SOCKS v5 call flow

1. Step 1-3: Open a TCP connection to the SOCKS5 Proxy.
2. Step 4-7: SOCKS messages are transported via the TCP connection established in phase (A). In the step 4-5, the client and server negotiate the SOCKS version and the authentication method. When it is used between the UE and UPF, the authentication method could select “No Auth”. In step 6-7 UDP ASSOCIATE procedure, the client sends the desired destination address and port to the SOCKS Proxy, and the SOCKS Proxy replies succeeded and BND.ADDR and BND.PORT where it must send UDP packets to be relayed. The destination address and port number in the UDP ASSOCIATE request message can be set to zero if the client is not in possession of these information at the time of the UDP ASSOCIATE.
3. User data transport phase. Each UDP datagram carries a UDP request header which includes the DST.ADDR and DST.PORT indicating the remote server IP address and port number.

The SOCKSv5 needs approximately 3 RTTs including one for TCP before the data transport, i.e. phase (A) and (B). As an optimized solution, SOCKS proxy information can be transported via NAS message to avoid phase (A) and (B) to reduce the RTT. One or more QUIC connections between the UE and the UPF may be established based on the procedure in clause 6.8.3. These QUIC connections can be encrypted or be NULL encryption. The following two possible solutions can be considered to support the NULL encryption QUIC connection, which needs further to be studied in SA3.

* Solution 1: TLS 1.3 can be extended to support the NULL encryption algorithm.
* Solution 2: The TLS layer is taken as optional for QUIC protocol, as the TLS authentication and encryption can be skipped when it is applied between the UE and UPF.

If the radio level security is enabled, it is proposed to use the NULL encrypted QUIC connection.

No matter transparent QUIC or non-transparent QUIC solution, the version information, transport parameters of the QUIC protocol applied by the QUIC proxy, can be sent to UE in QUIC connection establishment procedure via user plane, as defined in IETF draft-ietf-quic-transport [6]. Alternatively, the QUIC proxy information can also be sent to UE via NAS message in order to achieve 0-RTT QUIC connection establishment. In the QUIC proxy side, it will identify the QUIC traffic based on the packet filter and QUIC method indication from SMF via N4 rule and forward these packets to the target server after removing QUIC header. For the non-transparent QUIC solution, QUIC proxy needs to replace the target IP address with the remote Server IP address, in addition.

The protocol stack is defined in Figure 6.8.2-2, taking untrusted non 3GPP access as an example:



Figure 6.8.2-2: Protocol stack of QUIC

**QUIC connection between the UE and remote server:**

If the QUIC functionality is implemented by the application layer, between the UE and the server (i.e. remote host), there is no need to enable the QUIC proxy functionality in the UPF. These QUIC packets can directly be handled by ATSSS-LL as described above when the UPF knows this is a QUIC connection. For example, the PCF is aware that the application supports QUIC, the PCF may allow the traffic splitting per packet for a SDF by indicating only one packet flow in this SDF. Otherwise, it depends on the UPF to identify the QUIC packet from the other UDP packets, e.g. based on DPI analysis. When the UPF identifies the QUIC packets, the traffic switching or splitting per packet based on the steering mode and link performance measurement of PMF can be performed by the ATSSS-LL functionality. The PCF can be aware of the application transport protocol, i.e. QUIC protocol, based on the local policy or the protocol from AF, similar as the protocol from AF to PCRF as defined in TS 29.214 subclause 5.3.8.

### 6.8.3 Procedure

For the first case, i.e. QUIC connection is between the UE and the UPF, the signalling flow for a MA PDU Session establishment when the UE is not roaming, or when the UE is roaming and the PDU Session Anchor (PSA) is located in the VPLMN, is described as below.



Figure 6.8.3-1: QUIC based MA PDU Session establishment procedure

- In step 1, the UE provides a "MA PDU Request" indication in UL NAS Transport message and an ATSSS Capability indicating support of "QUIC Capability" in PDU Session Establishment Request message.

 The "MA PDU Request" indicates to the network that this PDU Session Establishment Request is to establish a new MA PDU Session and to apply the QUIC functionality, for traffic steering of this MA PDU session.

- In step 2, if the AMF supports MA PDU sessions, then the AMF selects an SMF, which supports MA PDU sessions, and forwards the MA PDU Session Establishment Request to the SMF.

- In step 3, if the MA PDU session is allowed and dynamic PCC is to be used for the MA PDU Session, the SMF sends an "MA PDU Request" indication and the ATSSS Capability of MA PDU Session to the PCF in the SM Policy Control Create message and. The ATSSS Capability includes the QUIC functionality.

 The PCF provides ATSSS Steering policy if the MA PDU session is allowed. The PCF provides PCC rules for the MA PDU session, i.e. PCC rules that include ATSSS policy control information, which includes the QUIC functionality and ATSSS-LL functionality indication if both QUIC functionality and ATSSS-LL functionality are supported. Additionally, the PCC rules may also indicate on whether the encryption of the QUIC connection is needed or not based on operator policy and subscription data or access type for this MA PDU session.

- In step 4, the SMF establishes the user-plane resources over the 3GPP access and/or non-3GPP.

- the N4 rules derived by SMF for the MA PDU session are sent to UPF and one or two N3 UL CN tunnels info may be allocated by the SMF or by the UPF. If the ATSSS functionality for the MA PDU Session indicates "QUIC functionality and ATSSS-LL functionality", the SMF includes QUIC functionality and ATSSS-LL functionality into the N4 rule to instruct the UPF to activate the QUIC functionality and ATSSS-LL functionality for the traffic. If the QUIC connection needs encryption or NULL encryption, the SMF also indicates it to the UPF.

- In step 5, the UPF allocates QUIC functionality information if the non-transparent QUIC functionality applied for this MA PDU session in the UPF. The UPF sends QUIC functionality information to the SMF. The QUIC functionality information includes the QUIC functionality IP address and UDP port number.

- In step 6, for the MA PDU session, the SMF includes an "MA PDU session Accepted" indication and PDU Session Establishment Accept message which includes ATSSS rules for MA PDU Session and the QUIC functionality information in the Namf\_Communication\_N1N2MessageTransfer message to the AMF and the AMF marks this PDU session as MA PDU session based on the received "MA PDU session Accepted" indication, same as defined in Rel-16 specifications.

- In step 8, the UE receives a PDU Session Establishment Accept message, which indicates to the UE that the requested MA PDU session was successfully established. This message includes the ATSSS rules for the MA PDU Session, which includes steering mode, the QUIC functionality and ATSSS-LL functionality indication and encryption or NULL encryption indication for the traffic.

- After step 8 in Figure 6.8.3-1, if the SMF was informed in step 2 that the UE is registered over both accesses, then the SMF initiates the establishment of user-plane resources over non-3GPP access too as specified in TS 23.502 [4] clause 4.22.2.1.

The last step above is not executed when the UE is registered over one access only, in which case the MA PDU Session is established with user-plane resources over one access only. How user-plane resources can be added over an access of the MA PDU Session is specified in TS 23.502 [4] clause 4.22.7.

For the second case, i.e. QUIC connection between the UE and remote server, the existing procedure as specified in TS 23.502 [4] clause 4.22.2 is applied.

### 6.8.4 Impacts on services, entities, interfaces and IETF protocols

This solution will impact the following entities in 5GS:

-PCF: Supports to authorize the QUIC and ATSSS-LL method for the SDF.

-SMF: Supports to select the UPF supporting both QUIC and ATSSS-LL functionality.

-UPF: Supports to establish the QUIC connection with UE.

-UE: Supports to establish the QUIC connection with UPF.

-5G-AN/ NG RAN: No impact.

This solution may impact IETF. As the current QUIC connection defined by IETF shall be encrypted based on the TLS 1.3, the NULL encryption QUIC connection requires IETF support.

\* \* \* \* End of changes \* \* \* \*