**3GPP TSG-WG SA2 Meeting #164 *S2-240xxxx***

**Maastricht, NL, 19 - 23 August, 2024 (revision of S2-2407619)**

**Source: Ericsson, Meta USA, InterDigital, Apple, Lenovo**

**Title: KI#2, Sol #26: Update to remove ENs**

**Document for: Approval**

**Agenda Item: 19.3**

**Work Item / Release: FS\_XRM\_Ph2 / Rel-19**

*Abstract: Resolves Editor’s Notes of Solution #26 in TR 23.700-70*

# 1. Introduction/Discussion

This solution addresses Key Issue #2 (Support XRM metadata identification for end-to-end encrypted XRM traffic).

In this pCR the remaining Editor’s notes are being address.

# 2. Text Proposal

It is proposed to introduce the following changes vs. TR 23.700-70.

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

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 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.503: "Policies and Charging control framework for the 5G System; Stage 2".

[5] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)", March 2004.

[6] IETF RFC 6904: "Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)".

[7] IETF RFC 9335: "Completely Encrypting RTP Header Extensions and Contributing Sources".

[8] IETF draft-ietf-avtcore-rtp-over-quic: "RTP over QUIC (RoQ)".

[9] IETF draft-ietf-moq-transport: "Media over QUIC Transport".

[10] IETF experimental draft-ietf-avtext-framemarking: "Frame Marking RTP Header Extension".

[11] IETF RFC 9000: "QUIC: A UDP-Based Multiplexed and Secure Transport".

[12] TR 26.926 v18.1.0: "Traffic Models and Quality Evaluation Methods for Media and XR Services in 5G Systems".

[13] TR 26.925 v18.1.0: "Typical traffic characteristics of media services on 3GPP networks".

[14] IETF RFC 9330: "Low Latency, Low Loss, and Scalable Throughput (L4S) Internet Service: Architecture.

[15] IETF RFC 9331: "The Explicit Congestion Notification (ECN) Protocol for Low Latency, Low Loss, and Scalable Throughput (L4S)".

[16] IETF draft-ietf-tsvwg-ecn-encap-guidelines-22: "Guidelines for Adding Congestion Notification to Protocols that Encapsulate IP".

[17] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[18] CableLabs DOCSIS MULPI: "Data-Over-Cable Service Interface Specifications DOCSIS 3.1, MAC and Upper Layer Protocols Interface Specification".

[19] IETF RFC 9332: "Dual-Queue Coupled Active Queue Management (AQM) for Low Latency, Low Loss, and Scalable Throughput (L4S)".

[20] 3GPP TS 26.522: "5G Real-time Media Transport Protocol Configurations".

[21] IETF [draft-ietf-tsvwg-udp-options:](https://datatracker.ietf.org/doc/draft-ietf-tsvwg-udp-options/) "Transport options for UDP".

[22] IETF RFC 6363: "Forward Error Correction (FEC) Framework".

[23] IETF RFC 6364: "Session Description Protocol Elements for the Forward Error Correction (FEC) Framework".

[24] IETF RFC 6681: "Raptor Forward Error Correction (FEC) Schemes for FECFRAME".

[25] IETF RFC 6682: "RTP Payload Format for Raptor Forward Error Correction (FEC) ".

[26] IETF RFC 6695: "Methods to Convey Forward Error Correction (FEC) Framework Configuration Information".

[27] IETF RFC 6816: "Simple Low-Density Parity Check (LDPC) Staircase Forward Error Correction (FEC) Scheme for FECFRAME".

[28] IETF RFC 6865: "Simple Reed-Solomon Forward Error Correction (FEC) Scheme for FECFRAME".

[29] IETF RFC 8680: "Forward Error Correction (FEC) Framework Extension to Sliding Window Codes".

[30] IETF RFC 8681: "Sliding Window Random Linear Code (RLC) Forward Erasure Correction (FEC) Schemes for FECFRAME".

[31] 3GPP TS 38.300: "NR; NR and NG-RAN Overall description; Stage-2".

[32] IETF RFC 8627: "RTP Payload Format for Flexible Forward Error Correction (FEC)".

[33] IETF RFC 7656: "A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources".

[34] S2-2210181: "Reply LS on further details on XR traffic".

[35] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes; Stage 3".

[36] 3GPP TS 38.415: "NG-RAN; PDU Session User Plane Protocol".

[37] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

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

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

[40] IETF draft-ietf-masque-quic-proxy-03: "QUIC-Aware Proxying Using HTTP".

[41] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".

[42] IETF RFC 5764:"Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)".

[43] IETF RFC 7983: "Multiplexing Scheme Updates for Secure Real-time Transport Protocol (SRTP) Extension for Datagram Transport Layer Security (DTLS)".

[44] IETF RFC 8872: "Guidelines for Using the Multiplexing Features of RTP to Support Multiple Media Streams".

[45] IETF RFC 9443: "Multiplexing Scheme Updates for QUIC".

[46] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

Editor's note: References [8], [9] and [10] cannot be formally referenced until published as RFC.

[47] IETF RFC 6040: "Tunnelling of Explicit Congestion Notification".

[48] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

\* \* \* \* Second change \* \* \* \*

6.26 Solution #26: PDU Set identification for end-to-end encrypted traffic

6.26.1 Key Issue mapping

This solution addresses Key Issue #2: "Support XRM metadata identification for end-to-end encrypted XRM traffic".

6.26.2 Description

This solution proposes to enable the support of PDU Set related handling for end-to-end encrypted traffic, first with a general tunnelling framework and then using QUIC as transport protocol and XRM metadata with XRM metadata in UDP tunnel packets as in-band communication between 5GS and the content-provider AS. The end-to-end XRM traffic can be RTP over QUIC, media over QUIC or any other XRM application protocol carried over QUIC.

The packets carrying XRM traffic are encapsulated within QUIC packets via QUIC streams to transport real-time data within a QUIC connection for a specific IP flow (represented by IP 5-tuple) and are encrypted through embedded QUIC security based on TLS 1.3.

The solution includes two parts: a general framework based on the use of any tunnel protocol with indicated set of characteristics and a solution realization based on UDP-connect.

NOTE 1: To ensure interoperability, the default encapsulation protocol shall be the UDP-connect as specified in clause 6.26.4.

6.26.3 General framework

The solution proposes to have a framework where fully encrypted packets from an application server are tunnelled via an encapsulation protocol between the UPF and the Application Server over the N6 reference point as shown in Figure 6.26.3-1.

****

**Figure 6.26.3-1: General framework for supporting PDU set identification for fully encrypted media packets**

The main steps of the solution comprise of the following elements:

1. An AF when requesting an AF session towards the 3GPP network (NEF) includes additional information indicating to the 3GPP network that the UPF can identify PDU-set information by inspecting the headers of an encapsulation protocol. The AF also including the address of the XR Video application server where the UPF will need to establish a connection using the encapsulation protocol.

NOTE 1: It is assumed that the 3rd party provider of the AF and the 3GPP network have SLA agreement on the type of encapsulation protocol to use between the UPF and AS over N6 reference point.

NOTE 2: To ensure interoperability, the default encapsulation protocol shall be the UDP-connect as specified in clause 6.24.3.2.

2. The PCF in the 3GPP network providing PCC rules where the PCC rules includes the information provided by the AF in step 1.

3. The SMF constructing N4 rules based on the PCC rules where the N4 rules include uplink and downlink Packet Detection Rules indicating to the UPF that:

a. for uplink packets sent from a specific UE (or any UE) to a specific application server the UPF would need to establish a connection using an encapsulation protocol and route the packet via the encapsulation protocol to the Application Server address.

b. For downlink packets received by the UPF over N6 configuration information indicating the UPF to:

i. Extract the encapsulated UDP packet from the received IP packet.

ii. Enable PDU set identification and retrieve XRM metadata from information contained within the encapsulation protocol.

iii. Routing the decapsulated UDP packet over a QoS flow with PSDB requirements within GTP signalling towards the RAN.

4. UPF that supports an encapsulation protocol client establishing a protocol session with a server once the UPF detects that an uplink packet is sent towards a specific destination address.

NOTE 3: If the UPF determines that there is already a tunnel open towards the XR application server (e.g. from another UE XR session), the UPF can forward the UE packet via the existing connection. The decision is based on UPF implementations or operator configuration, although it may affect load balancing implementation at the Application Server.

5. The Application Server sending downlink packets via the encapsulation protocol and includes additional XRM metadata provided in-band within the encapsulation protocol to assist the UPF to identify XRM metadata.

6. The UPF identifying XRM metadata of PDUs of PDU sets based on the information provided within the encapsulation protocol and routing the packet via a QoS flow with PSDB requirements based on the N4 rules including within the GTP-U header XRM metadata for each PDU.

NOTE 4: If not released by the Application Server, it is up to UPF implementation when the tunnelled connection is released, e.g. when the UPF determines no traffic is routed via the tunnelled connection for a specific period of time then the connection is released. Other solutions are FFS.

6.26.3.1 General procedure

Details steps of the procedure are shown in Figure below:

****

**Figure 6.26.3.1-1: General procedure for supporting PDU set identification for fully encrypted media packets**

1. An AF requests to establish an AF session with QoS by invoking the Nnef\_AFSessionWithQoS Create service operation as described in clause 4.15.6.6 of TS 23.502 [3] including PDU Set QoS parameters for the XR service. The AF additionally includes information to enable an encapsulation protocol connection between the UPF and AS and the address of the server where the UPF can establish the encapsulation protocol session.

Not shown in the Figure the NEF authorizes the request and forwards the request to the PCF by invoking an Npcf\_PolicyAuthorization\_Create request including the information provided by the AF.

NOTE 1: Several applications hosted on the same Application Server may be distinguished by the UDP 5-tuple negotiated in the SDP offer/answer negotiation, which can be provided by the AF as Flow description. This may allow the AF to specify different PDU Set QoS Parameters for different applications or no PDU Set QoS Parameters at all. If the 5-tuple is not available, they can be distinguished by mechanisms not described in this solution.

2. The PCF creates PCC rules taking into account the PDU Set QoS parameters as described in clause 6.1.3.22 of TS 23.503 [4]. The PCC rule also includes the encapsulation protocol details and server address.

3. The SMF binds the PCC rules to a new QoS flow, determines the applicable QoS Profile and determines N4 rules including a QoS Enforcement Rule with PDU Set marking indication, a Packet Detection Rule including the Packet Detection Information and a Protocol Description for QUIC packets including XRM metadata in XRM metadata and a Forwarding Action Rule with an indication to establish the UDP tunnel and the FQDN/IP address + port number of the AS. Alternatively, the SMF may be configured to support PDU Set QoS handling without receiving PCC rules from a PCF. The downlink Quality Enforcement rule includes information to enable PDU set inspection and extract PDU-set information from information contained within the encapsulation protocol.

4. The N4 rules are sent to the UPF. The FAR includes an indication to establish a UDP tunnel together with the address of the AS.

The SMF sends the QoS profiles to the NG-RAN via AMF and QoS rules to the UE via AMF and NG-RAN.

5. An application in the UE is triggered to connect to the AS

6. The application sends packets for the end-to-end encrypted connection via uplink over the 3GPP network

7. The UPF inspects the packet and determines that there is a matching PDR rule with a FAR indicating to establish an encapsulation protocol session to a server address and route the uplink packet via the encapsulation protocol

8. The UPF sends a session request to establish a connection using the encapsulation protocol procedure

9. The server acknowledges

10. The UPF encapsulates the uplink packet within the encapsulation protocol header.

11. The session packet is sent to the AS via N6

12. Further downlink and uplink packets may be routed to fully encrypt the connection between the UE and AS

13. The Application Server determines PDUs belonging to PDU set and adds XRM metadata within the encapsulation protocol

14. The UDP packet is sent via the encapsulation protocol to the UPF

15. The UPF extracts the UDP packet and determines XRM metadata using the XRM metadata provided within the encapsulation protocol.

6.26.4 PDU Set based QoS handling using UDP-connect

The solution is based on the following principles:

- To receive PDU Set information from the AS in a secure way, the UPF establishes a UDP tunnel to the AS by sending an HTTP request with the "connect-udp" upgrade token to an HTTP proxy integrated in the AS and indicating the capability to receive XRM metadata associated with end-to-end XRM PDUs.

- XRM metadata consists of the PDU Set Sequence Number, PDU Set Size and Importance, PDU Sequence Number within the PDU Set and End of Data Burst indication.

NOTE 1: HTTP datagram formats do not need IETF standardization. If HTTP header fields are used to indicate support for the specific format, the names of such fields need to be registered with IANA. The specific datagram format will be specified by CT working groups.

- If the end-to-end connection between the UE and the Application Server is based on QUIC. To avoid re-encapsulation and re-encryption, all XRM payload packets shall be forwarded using the Forwarded Mode in QUIC-Aware Proxying using HTTP [40]. The XRM metadata is encoded into the XRM packets by use of a packet transform that is applied to proxied QUIC packets. The packet transform changes the QUIC packet such that the XRM metadata is inserted into the QUIC packet. The AS encrypts the XRM metadata and inserts it to the packet, and when the UPF receive the QUIC packet it decrypts the XRM metadata and reconstructs the original packet. The Forwarded Mode can be applied to short header QUIC packets after registration of the Connection ID. If the end-to-end connection is not based on QUIC, the XRM payload packets can be sent together with metadata within HTTP Datagrams using connect-udp without QUIC-Aware Proxying.

NOTE 2: For QUIC end-to-end connections, QUIC-Aware Proxying using Tunnelled Mode can be used with the disadvantage of double encryption as XRM payload packets are encrypted within the QUIC connection.

NOTE 3: The framework for packet transforms is described in [40]. Packet transforms are used to transform proxied packets that are being forwarded instead of encapsulated. The use of a specific transform is negotiated in the connect-udp request and response sequence. New packet transforms do not require IETF standardization, but the name of the packet transform must be registered with IANA. The specific packet transform will be specified by CT working groups.

Specification of a new packet transform is required for this solution. The 3GPP can specify this new packet transform to function within the framework defined in IETF for QUIC Aware Proxying [40]. With this solution, a packet is transformed by inserting a length field directly after the connection ID of the forwarded end-to-end packet. The XRM metadata follows directly after the length field. The XRM metadata is encrypted and integrity protected, using a shared key that is exchanged during the negotiation of the transform, and an initialization vector that is obtained from the end-to-end encrypted QUIC packet. The length field indicates the offset at which the end-to-end encrypted QUIC payload starts. For integrity protection of the XRM metadata a MAC is inserted after the Metadata, the MAC covers both the Metadata and the Metadata length field. The use of an Initalization Vector containing data from the end-to-end encrypted packet binds the protected XRM metadata to the end-to-end packet such that it makes replay- or substitution attacks virtually impossible.

NOTE 3: A new packet transform specified by 3GPP will be registered in the relevant IANA registry being defined in [40].

NOTE 4: Details of the packet transform solution and the relevant cryptographic algorithms will be agreed with SA WG3.

NOTE 5: In case of CID collision the connection will be abnormally released.

****

**Figure 6.26.4-1: XRM metadata contained in transformed XRM Payload QUIC packet**

- In this solution the UPF is responsible for registering Connection IDs (CIDs) to be used for QUIC aware forwarding. From the first long header packet it sees originated from the UE, the UPF extracts the source connection ID of the end-to-end client, which it sends in a REGISTER\_CLIENT\_CID message towards the AS Masque proxy. Similarly, from the first long header packet originated from the AS the UPF will extract the source connection ID of the end-to-end server, which it sends in a REGISTER\_TARGET\_CID message towards the AS Masque proxy. Note that prior to registrations being completed, packets are sent in tunnelled mode, and that all long header packets are sent in tunnelled mode.

The MASQUE endpoints cannot see the negotiation of new CIDs of the end-to-end connection, but they will observe a new CID when it is used. In the mobile network, the IP address should not change (or at least not without UPF’s knowledge), so even if the CID changes, the MASQUE endpoints can still associate the incoming packets to an existing MASQUE tunnel based on the 4-tuple and send them in tunnel mode. Note that short headers include only the Destination CID in cleartext.

If the AS changes its CID, the UPF detects the change of the Destination CID in a subsequent short header packet originated from the UE and it will send this packet in tunnelled mode as no mapping to a VCID is registered (yet). In parallel it can extract the CID from the packet (assuming a CID length that is equal to what was sent in the long header packets) and send a REGISTER\_TARGET\_CID message with this new CID to request a new CID to VCID mapping from the AS proxy. Similarly, if the UE changes its CID, the AS Masque proxy detects a new Destination CID in a packet coming from the AS and it will send the packet in tunnelled mode towards the UPF since CID to VCID mapping has not been requested yet for this CID. When the UPF receives a packet from the tunnel that has a new Destination CID, it can extract the new CID from the packet and send it in a REGISTER\_CLIENT\_CID message to request a new CID to VCID mapping from the AS proxy.

As soon as the MASQUE endpoints get the new VCID mapping, they can start using the forwarded mode again. This mechanism can be applied independently for each direction. Sending any packets in tunnel mode in the middle of a connection is not a problem as each MASQUE endpoint can switch between modes at any time. Note that most QUIC implementations do not change the CID without a concrete reason.

If for any reason, the CID cannot be reliably extracted, packets are sent in tunneled mode (e.g. as per Solution#24). If UEs use zero-length CIDs the packets shall be sent in tunneled mode.

- The AF sends AF session request message including QoS requirement and assistance information for the media traffic to the NEF/PCF including:

- The QoS requirements that contain the PDU Set based QoS parameters

- Traffic description that includes the matching condition: IP filter or application ID

- Protocol Description that indicates the specification for PDU Set Information.

- FQDN address of the target AS.

6.26.4.1 PDU Set based QoS handling for end-to-end encrypted XRM traffic

****

**Figure 6.26.4.1-1: Procedure for PDU Set based QoS handling for QUIC-based encrypted traffic**

The process includes the following steps:

1. PDU Session Establishment procedure (defined in clause 4.3.2.2.1 of TS 23.502 [3]) is performed.

2. The AF sends Nnef\_AFsessionWithQoS\_Create request to the PCF/NEF as defined in clause 4.15.6.6 of TS 23.502, providing PDU Set based QoS requirement and assistant information for traffic detection. It provides an indication of PDU Set Information Datagrams in the Protocol Description and the Address of the AS to establish the UDP tunnel with the connect-udp (or connect-ip as an alternative).

NOTE 1: Several applications hosted on the same Application Server may be distinguished by the UDP 5-tuple negotiated in the SDP offer/answer negotiation, which can be provided by the AF as Flow description. This may allow the AF to specify different PDU Set QoS Parameters for different applications or no PDU Set QoS Parameters at all. If the 5-tuple is not available, they can be distinguished by mechanisms not described in this solution.

The PCF generates PCC Rules based on the information provided by the AF and/or local policies, as defined in clause 6.1.3.27.4 of TS 23.503 [4] and including a request to identify and mark the PDU Set information on the end-to-end encrypted media traffic.

3. PCF forwards the PCC Rules for end-to-end encrypted XRM traffic to the UPF within SM Policy Association Establishment/Modification

4. The SMF binds the PCC rules to a new QoS flow, determines the applicable QoS Profile and determines N4 rules including a QoS Enforcement Rule with PDU Set marking indication, a Packet Detection Rule including the Packet Detection Information and a Protocol Description for PDU Set Information Datagrams and a Forwarding Action Rule with an indication to establish the UDP tunnel and the FQDN for the AS. Alternatively, the SMF may be configured to support PDU Set QoS handling without receiving PCC rules from a PCF.

The SMF sends the N4 rules including PDR, QER and FAR to the PSA UPF. The FAR includes an indication to establish a UDP tunnel together with the address of the AS.

NOTE 2: A PSA UPF with proxy capability need to be selected for the PDU Session that supports receiving in-band assistance information. How to select PSA UPF can be left to normative phase if the solution can be concluded.

NOTE 3: Impacts for URSP rule providing (e.g. with regard to UE capability) is left to normative phase if the solution can be concluded.

5. The SMF sends the QoS profiles to the NG-RAN via AMF and QoS rules to the UE via AMF and NG-RAN.

6. The UE sends packets on an QUIC connection towards the AS to enable the end-to-end encryption of the XRM traffic.

7. The UPF matches the PDR for the end-to-end encrypted QUIC connection for XRM application using the Packet Detection Information and determines that PDU Set identification and marking is to be applied based on the Quality Enforcement Rule linked to the Packet Detection Rule.

NOTE 4: Traffic not belonging to an XRM application or not supporting XRM metadata marking will match a PCC Rule with no UDP tunnel establishment indication. Even if both applications are hosted by the same IP address in the AS, the 5-tuple or Application Id is different.

8. Based on the contents of the FAR, the UPF decides to establish a QUIC connection to the AS and sends a connect-udp to the target AS identified by its FQDN to establish a UDP tunnel.

9. The UPF forwards the QUIC packet sent by the UE in step 7 towards the AS using the UDP tunnel.

NOTE 5: Packets addressed to the Application Server but matching PDRs connected to FARs without the UDP tunnel establishment indication will not be forwarded through the UDP tunnel, even if already established.

10. The AS and UE complete the end-to-end QUIC connection establishment with packets forwarded through the UDP tunnel.

11. The AS/HTTP/3 proxy inserts PDU Set information as XRM metadata into the XRM payload packets and applying a packet transform to the proxied QUIC packets. The AS encrypts the XRM metadata and inserts it to the packet, the UPF decrypts the XRM metadata and reconstructs the original packet.

12. UPF takes the QUIC packets from the UDP tunnel and sends them to the NG-RAN, adding the PDU Set information from the XRM metatdata s to the GTP-U extension header.

13. The NG-RAN sends the media packets using the required PDU Set QoS parameters.

14-15. When the end-to-end QUIC connection is closed, the Application Server also closes the UDP tunnel with the UPF. Alternatively, the UPF may close the UDP tunnel by using an inactivity timer.

6.26.5 Impacts on services, entities and interfaces

**AF:**

- Provides the Protocol Description with an indication of HTTP datagrams for PDU Set Information within Nnef\_AFsessionWithQoS\_Create request.

- Provides the FQDN address of the target AS within Nnef\_AFsessionWithQoS\_Create request.

**PCF:**

- Receives the Protocol Description and the FQDN of the AS from the AF.

- Generates PCC rules with a UDP tunnel set up indication and the FQDN of the target AS.

**SMF:**

- Sends N4 rules to the UPF including PDRs, QERs and FARS with PDU Set identification and marking indication and a UDP tunnel setup indication and FQDN of the target AS.

**UPF:**

- Establishes a UDP tunnel when matching an UL PDR linked to a FAR with UDP tunnel set up indication, if the tunnel is not already established.

- Receives HTTP datagrams with encrypted XRM metadata together with QUIC payload from the AS through the UDP tunnel and extracts the original QUIC payload packet and the encrypted XRM metadata and decrypts it.

- Sends the QUIC packets to the NG-RAN together with the PDU Set information in the XRM metadata from the HTTP datagrams in the GTP-U header extension.

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