**3GPP TSG-SA2 Meeting #164 *S2-2408806***

**Maastricht, Netherlands, 19 - 23 August 2024 (revision of S2-2407859)**

**Title: [draft]** LS on XRM metadata exchange between 3GPP Core and an Application server

**Response to:**

**Release:** Rel-19

**Work Item:** FS\_XRM\_Ph2

**Source:** Nokia, Will be SA2

**To:** IETF Multiplexed Application Substrate over QUIC Encryption WG chairs: [Dennis Jackson](https://datatracker.ietf.org/person/ietf@dennis-jackson.uk), [Eric Kinnear](https://datatracker.ietf.org/person/ekinnear@apple.com).

**Cc:** [liaison-coordination@iab.org](mailto:liaison-coordination@iab.org), [3gpp-liaison@ietf.org](mailto:3gpp-liaison@ietf.org).

**Contact Person:**

#### Name: Laurent Thiebaut

E-mail Address: [Laurent.thiebaut@nokia.com](mailto:Laurent.thiebaut@nokia.com)

**Send any reply LS to: 3GPP Liaisons Coordinator,** [**mailto:3GPPLiaison@etsi.org**](mailto:3GPPLiaison@etsi.org)

**Attachments:**

1. **Overall Description:**

**Background information**

3GPP SA2 is working to provide dedicated Quality of Service (QoS) for XRM (eXtended Reality) traffic flows over 3GPP networks (5G); for this purpose, a 3GPP network needs inband (along with the packets) certain metadata about the structure and characteristics of the application media content in the traffic flows. The following metadata has been defined in 3GPP Release 18:

PDU Set**:** One or more PDUs (for IP based traffic a PDU is an IP packet) carrying the payload of one unit of information generated at the application level (e.g. frame(s) or video slice(s) etc. for eXtended Reality (XR) Services).

End PDU of the PDU Set

PDU Set Importance [PSI]

PDU Set Sequence Number [PSSN]

PDU Sequence Number within a PDU Set [PSN]

PDU Set Size [PSSize]

End of Data Burst [EDB] ( A set of multiple PDUs generated and sent by the application in a short period of time)

It is also Important to note that the set of XRM metadata information to be made available to the 3GPP network (UPF) will be extended in the future (as part of 3GPP R19 and beyond e.g. to deal with media multiplexing in an UDP/IP flow).

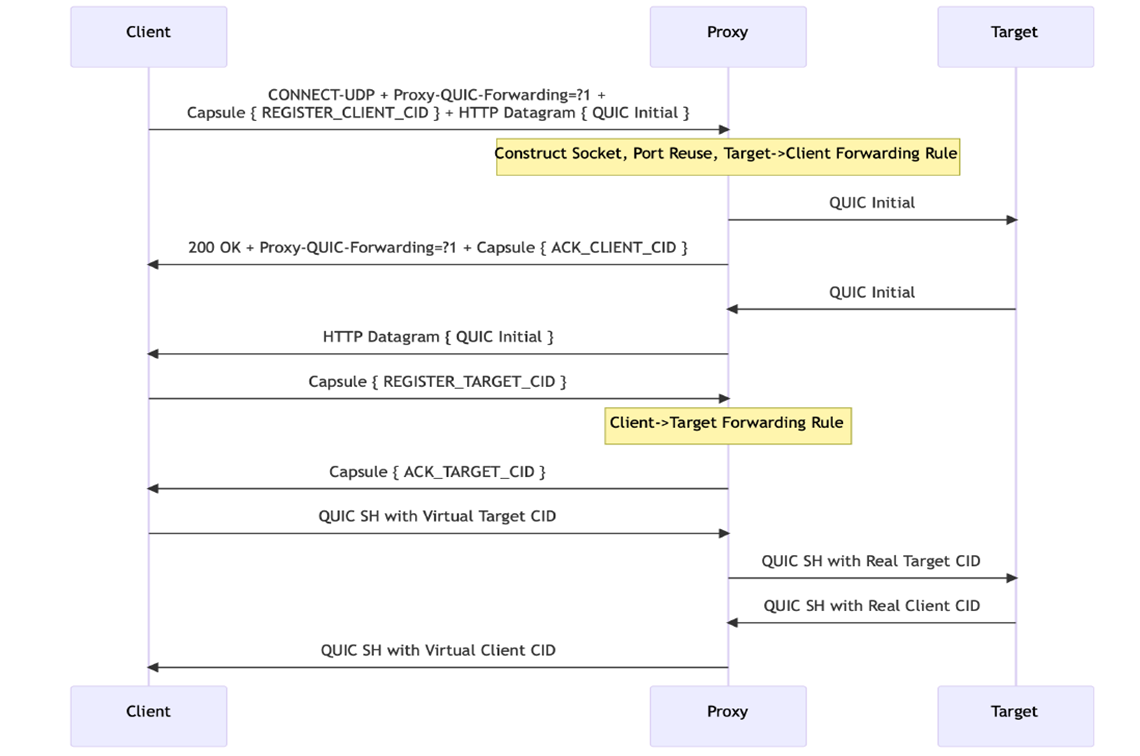
For RTP based traffic PDU Set and End of Data Burst information has been defined by 3GPP to be carried by a new RTP header extension. The same can be followed for any extended metadata. When XRM traffic is carried encrypted end to end (between UE and XRM application server) in protocols which do not allow unencrypted header extensions, additional mechanisms need to be defined for 3GPP networks (UPF) to be able to access to this XRM metadata information while ensuring that actual XRM traffic remains protected end to end and that entities beyond the 3GPP network (UPF) cannot read or modify the XRM metadata information either.

**Questions related with** QUIC-Aware proxying

To support 5G Core UPF access to XRM metadata, 3GPP (TR 23.700-70) is considering to use Proxy-UDP-in-HTTP/3 per RFC 9298 + QUIC-Aware proxying per draft-ietf-masque-quic-proxy.

A possible deployment of the feature would be where the draft-ietf-masque-quic-proxy Client would be in the UPF and thus not in the same entity than the end QUIC client. UE and UPF would be connected by IP networking as specified by 3GPP with UE acting as an IP host and UPF as an IP Router. Metadata about the end-to-end (UE to Target) QUIC connection would be carried between UPF and Proxy. The arrangement between Proxy and Target (the QUIC server acting as the Application Server for the XRM traffic) is not in scope of 3GPP.

UE



UPF

For this kind of deployment following questions have been asked that require detailed expertise on draft-ietf-masque-quic-proxy:

QUIC allows new end-to-end CID values to be negotiated between the UE (QUIC client) and the Target (QUIC Server) anytime during the lifetime of the end-to-end QUIC connection. When this happens, the UPF would not be able to learn the actual new end-to-end CID values But the UPF can detect new end-to-end CID values are used in QUIC packets it receives with short headers, even though UPF can only do this detection based on the length of the initial end-to-end CID having been used (as QUIC packets with short headers do not contain CID length).Once it has detected a new end-to-end CID is being used, the UPF acting as a QUIC-Aware proxying client, can negotiate the usage of a new virtual CID to be associated with the subset of the new end-to-end CID it has detected.

The question is on whether IETF sees any issue with this mechanism?

1. **Actions:**

**To IETF Multiplexed Application Substrate over QUIC Encryption WG:**

**ACTION:** SA2 kindly asks IETF Multiplexed Application Substrate over QUIC Encryption WG to answer to the questions above.

1. **Date of Next TSG-SA WG2 Meetings:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | DATES | LOCATION | CTRY |
| SA2#165 | October 14th – 18th, 2024 | Hyderabad | India |
| SA2#166 | November 18th –22nd, 2024 | Orlando | USA |

**Please see** [**https://portal.3gpp.org/Meetings?tbid=375&SubTB=385#/**](https://portal.3gpp.org/Meetings?tbid=375&SubTB=385#/)