**3GPP TSG-CT WG3 Meeting #142 *C3-253572***

**Gothenburg, SE, 25 - 29 August 2025 (Revision of C3-253088)**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0195** | **rev** | **1** | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | N6 e2e encryption traffic update |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** | C3 |
|  |  |
| ***Work item code:*** | XRM\_Ph2 |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** |  |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | The following Media related information editor’s notes are removed:1. Editor's Note: 3gpp-Connect-Req-Inband-Info header and 3gpp-Connect-Resp-Inband-Info header need to be IANA registered.

There is no need to IANA registration required for HTTP header in 3GPP as shown in [Hypertext Transfer Protocol (HTTP) Field Name Registry](https://www.iana.org/assignments/http-fields/http-fields.xhtml). |
|  |  |
| ***Summary of change:*** | As there is no header addition for IANA, the corresponding editor note is removed.The zero length of Protected Media Related Information usage is explained. The typo are fixed. |
|  |  |
| ***Consequences if not approved:*** | The open issue in N6 e2e encrypted traffic handing is still open. |
|  |  |
| ***Clauses affected:*** | 22.3.2, 22.3.3, 22.3.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* \* First Change \* \* \* \*

### 22.3.2 Sending Media Related Information using proxying UDP in HTTP Datagram

To establish a connect-UDP tunnel as defined in IETF RFC 9298 [64], the HTTP client in the UPF shall include in the HTTP/3 CONNECT request:

a) the :protocol pseudo-header set to connect-udp; and

b) the 3gpp-Connect-Req-Inband-Info header defined in Annex A.3 with the intended-inband-purpose parameter set to "MRI".

EXAMPLE 1: 3gpp-Connect-Req-Inband-Info header in HTTP CONNECT request message for the format that includes the media related information in the HTTP Datagram payload:

3gpp-Connect-Req-Inband-Info: intended-inband-purpose=MRI

Upon successfully establishing the connection, the HTTP server (AS proxy) shall return a 2XX response including the 3gpp-Connect-Resp-Inband-Info header defined in Annex A.3 with:

a) the inband-purpose parameter set to "MRI" indicating that the AS will send Media Related Information as defined in clause 22.2, in HTTP Datagrams; and

b) the context-id parameter set to a non-zero odd value registered by the AS for the Context ID that will be used in HTTP Datagrams carrying Media Related Information.

EXAMPLE 2: 3gpp-Connect-Resp-Inband-Info header in HTTP CONNECT response message indicating successfully established connection with the registered Context ID (decimal) value 7:

3gpp-Connect-Resp-Inband-Info: inband-purpose=MRI; context-id=0b111

Upon receipt of the successful 2XX response as per IETF RFC 9298 [64], the UPF shall consider that the UDP tunnel is established to receive HTTP Datagrams carrying Media Related Information with the AS registered Context ID, received in the 3gpp-Connect-Resp-Inband-Info header.

If the HTTP client in the UPF chooses to reuse the QUIC connection to the HTTP server for multiple UEs, the UPF shall open a different QUIC stream for the HTTP/3 CONNECT request issued for each UE.

The HTTP client in the UPF may use different QUIC connections to the HTTP server for multiple UEs, each connection with a separate TLS security context as per IETF RFC 9114 [65].

When the Media Related Information is encapsulated in HTTP Datagrams of the connect-UDP tunnel, then the HTTP server (AS proxy) shall encode the HTTP Datagram payload format as below:

a) Context ID with format defined in IETF RFC 9298 [64], set to an odd number, derived as per the above procedure; and

Editor's Note: The description for Context ID and ABNF is FFS.

b) a payload containing:

1) Media Related Information with the format as defined in clause 22.2; and

2) UDP proxying payload.

Upon receipt of the HTTP Datagram with the Context ID registered as the value indicated in the 3gpp-Connect-Resp-Inband-Info header, the UPF shall extract the Media Related Information from the HTTP Datagram payload for DL transmission in the GTP-U header as defined in 3GPP TS 23.501 [2].

NOTE: The UDP proxying payload of the HTTP Datagram payload contains application data which is end-to-end encrypted between the UE and the Application Server.

\* \* \* \* Next changes \* \* \* \*

### 22.3.3 Sending Media Related Information using transport options for UDP

Upon establishment of a connect-UDP tunnel as defined in IETF RFC 9298 [64], if the Media Related Information is encapsulated in the transport options for UDP draft-ietf-tsvwg-udp-options [67], then the HTTP server shall include the Media Related Information in a UDP option of the outer UDP header of the connect-UDP tunnel. The UDP option for the Media Related Information shall contain:

1) one octet Kind field with the value "TBD" from the set of the UNASSIGNED values defined in draft-ietf-tsvwg-udp-options [67], indicating the UDP option is for the Media Related Information;

Editor's Note: The value "TBD" from the UNASSIGNED values defined in draft-ietf-tsvwg-udp-options [67] is to be IANA registered for the purpose of indicating that the UDP option includes the Media Related Information.

2) a length field, indicating the length of the UDP option in octets, as defined in draft-ietf-tsvwg-udp-options [67] where the length field shall be one octet; and

NOTE: The IP layer fragmentation is not allowed for UDP Datagrams according to IETF RFC 9000 [68] and the maximum size of one or more QUIC packets together with the UDP option within the UDP Datagram is limited to the Maximum Transmission Unit (MTU) size for the Ethernet PDU which is 1500 bytes. Therefore, the UDP option is kept to the maximum of 255 octets for QUIC packets.

3) the Media Related Information as defined in clause 22.2.

The Media Related Information shall be encrypted between the HTTP server and the HTTP client in the UPF.

Editor's Note: Details about format, encoding and encryption are to be further specified.

Upon receipt of the encrypted UDP option with Media Related Information, the UPF shall extract the Media Related Information from the UDP option for DL transmission in the GTP-U header as defined in 3GPP TS 23.501 [2].

\* \* \* \* Next changes \* \* \* \*

### 22.3.4 Sending Media Related Information using QUIC-aware proxying using HTTP

If the media traffic is transmitted over QUIC between the AS and the UE, the UPF (acting as client) and the AS (acting as UDP proxy) may negotiate to use the dedicated QUIC Connection IDs and packet transform in Forwarded Mode to avoid re-encapsulation and re-encryption as defined in IETF draft-ietf-masque-quic-proxy [67]. In case of multiple UEs using the same QUIC connection between the UPF and the AS, for each UE the UPF shall initiate a new HTTP CONNECT request to associate each UE with a separate Connection ID for mapping to a Virtual Connection ID as described in in IETF draft-ietf-masque-quic-proxy [67].

As described in IETF draft-ietf-masque-quic-proxy [67], the AS may still send some packets using the tunnelled mode even when the UPF and the AS have negotiated to use Forwarded Mode (e.g. during the initial media exchange with media related information from the AS to the UPF until it is possible to start using Forwarded Mode). Packets sent in tunnelled mode shall be encoded in HTTP Datagrams as defined in clause 22.3.2. Packets sent using Forwarded Mode shall be encoded as defined in this clause.

During the HTTP CONNECT method as described in IETF draft-ietf-masque-quic-proxy [67], in addition to what is required according to clause 22.3.2:

a) the UPF shall insert 3gpp:media-related-info-transform in the accept-transform parameter of the proxy-quic-forwarding header field in the HTTP CONNECT request; and

b) the AS shall indicate 3gpp:media-related-info-transform in the transform parameter of the proxy-quic-forwarding header field in the HTTP CONNECT successful response.

When the Media Related Information are transformed in the QUIC short header as per IETF RFC 9000 [68], then the 3gpp:media-related-info-transform shall be used to encode the transformed QUIC packet as shown in Figure 22.3.4-1 (using the notational conventions defined in section 1.3 of IETF RFC 9000 [68]).

Transformed QUIC Packet {

 Header Form (1) = 0,

 Fixed Bit (1) = 1,

 Spin Bit (1),

 Reserved Bits (2),

 Key Phase (1),

 Packet Number Length (2),

 Destination Connection ID (0..160),

 Length of Protected Media Related Information(8)

 Protected Media Related Information (..),

 Packet Number (8..32),

 Packet Payload (8..),

}

Figure 22.3.4-1: Transformed QUIC Packet with Media Related Information Container as per 3gpp:media-related-info-transform

In Figure 22.3.4-1:

a) Destination Connection ID shall be set to the mapping Virtual Connection ID;

b) the length of the protected Media Related Information shall be encoded in the number of bytes;

c) Protected Media Related Information shall be the output of the security algorithm defined in 3GPP TS 33.501 [59] which takes as an input the Media Related Information container, defined in clause 22.2. In case of the length of the protected media related information is zero, the Protected Media Related Information shall not be present; and

d) Packet Number and Packet Payload shall be set to the (end-to-end protected) packet number and the packet payload of the end-to-end packet.

Editor's Note: IANA registration of the 3gpp:media-related-info transform is needed.

Editor's Note: The details on the encoding of Protected Media Related Information based on SA3 is FFS.

If the Media Related Information is missing, the length of Protected Media Related Information shall be set to zero and the Protected Media Related Information field shall be omitted.

\* \* \* \* End of Changes \* \* \* \*