**3GPP TSG-SA2 Meeting #165 *S2-240xxxx***

**Hyderabad, India, 14 – 18th October 2024 (revision of S2-240)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** |  | **rev** | **-** | **Current version:** | **19.1.0** |  |
|  |
| *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:***  | Usage of UDP-Connect for Handling of end-to-end encrypted XR flows |
|  |  |
| ***Source to WG:*** | Nokia |
| ***Source to TSG:*** | S2 |
|  |  |
| ***Work item code:*** | XRM\_Ph2 |  | ***Date:*** | 2024-10-04 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-19 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA plenary approved conclusions in 23.700-70 clause 8.2  |
|  |  |
| ***Summary of change:*** | Add a high level description of The UDP-Connect mechanism defined to support XRM metadata detection by UPF when XR traffic is encrypted between UE and AS |
|  |  |
| ***Consequences if not approved:*** | conclusions in 23.700-70 clause 8.2 are not supported by normative work |
|  |  |
| ***Clauses affected:*** | 5.37.X.2 (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  |  |
| ***affected:*** |  | **x** |  Test specifications |  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** | This CR should be implemented after CR xxx |
|  |  |
| ***This CR's revision history:*** |  |

*FIRST CHANGE ALL text is new*

5.37.X.2 Usage of UDP-Connect in order to Handle end-to-end encrypted XR flows

5.37.X.2.1 Usage of only UDP-Connect

Proxy UDP in HTTP per RFC 9298 [xx1] may be used to support secured delivery of XRM metadata from AS to UPF. The mechanisms described in this clause apply when the AS is collocated with the UDP Proxy defined in RFC 9298 [xx1].

NOTE 1: This does not preclude potential deployments where there is cascading of UDP proxies but these potential deployments are not further addressed in this specification.

A UDP tunnel using UDP-Connect may be established between the UPF and the AS as follows:

- the AF may provide the Protocol Description for XRM metadata for encrypted traffic including an indication of support of UDP-Connect, and the corresponding AS address together with corresponding QoS requirements. This is done using the AF session with QoS procedure (as defined in clause 4.15.6.6 of TS 23.502 [3]) , and meant to support the establishment of a UDP tunnel with the connect-UDP upgrade token between the UPF and the AS.

Editor’s Note: whether AF session with QoS procedure allows to negotiate the format of the XRM metadata delivery over UDP-Connect

- The PCF generates a PCC rule including corresponding information.

- The SMF provides N4 rules to the UPF including the corresponding information.

- In the uplink direction, PDR and FAR rules are used to detect XR flow subject to Usage of UDP-Connect and to associate these flows with UDP-connect based proxying.

- In the downlink direction, PDR rules are used to detect XR flows.

- The UPF supports the HTTP/3 Client functionality, which establishes a UDP tunnel to the AS (where HTTP/3 Proxy operates) with the connect-UDP upgrade token when the UPF detects the start of a new UE flow towards the AS.

NOTE 2: When many UEs served by the same UPF have an encrypted XRM connection towards the same XRM AS, the UPF can determine to use a common single UDP-Connect tunnel with that AS.; The UPF needs to ensure it can De multiplex DL traffic from the AS to be able to route this DL towards the PDU Session (GTP-u tunnel) of the correct UE. For this purpose, the UPF can for example associate each UE’s PDU Session with a corresponding QUIC stream

- the UPF shall use context id =0 for uplink HTTP datagram payloads. The UPF determines a non-zero context ID for downlink HTTP datagram payload that during the tunnel creation, the UPF shall register with AS and associate with the format to be used for Downlink HTTP datagram.

 Downlink HTTP datagram payload consists of context ID, XRM metadata length, XRM metadata, and XRM data.

NOTE: This HTTP datagram payload will be further defined by CT groups;

 NOTE 3: If there is no more traffic using an established UDP-tunnel, the UPF can use implementation mechanisms such as idle timer to close a UDP-Connect stream or a UDP-Connect association.

When UDP tunnel using UDP-Connect has been established PDU(s) are handled as follows:

- Downlink PDU(s) received by UPF on N6 interface contain encrypted E2E XRM media along with XRM metadata. XRM metadata is encrypted between UPF and AS

- SMF instructs UPF on what packet should be captured using PDR rules and what action to be made on the detected packeted using Forwarding Action Rule.

- For DL traffic, UPF identifies the XRM metadata from the HTTP datagrams, and uses these XRM metadata to ensure relevant Qos is delivered to the PDU; This includes marking the PDU Set Information into GTP-U header as described in clause 5.37.5.2. When UPF receives DL packets over the UDP tunnel from AS, the UPF shall send over right PDU session towards UE. The UPF shall remove the context ID, XRM metadata length, XRM metadata in the data sent towards the UE .

- When UE sends UL packets carrying XRM data that is encrypted between UE and AS to the AS, the UPF sends those packets over the UDP tunnel[xx1].

XRM metadata may carry:

- PDU set Information as defined in clause 5.37.5.2 ,

- end of data burst as defined in clause 5.37.8.3,

- Source (SSRC), Payload Type (PT) and RTP-M header fields in RTP header [185] to detect multiplexed flows as defined in clause 5.37.y.

- Burst size as defined in clause 5.37.z;

- data boosting triggered by AS as defined in clause 5.37.w;

##### 5.37.X.2.2 Usage of UDP-Connect coupled with QUIC-Aware-proxying

Editor’s Note: the whole content of this clause is FFS and depends on IETF feedback

Editor’s Note: the whole content of this clause is still very draft

When UDP-Connect tunnelling is used for XRM traffic using QUIC, the double encryption of XRM traffic (once via QUIC between UE and AS and another time in encapsulation between UPF and AS) may be avoided using QUIC aware proxying with HTTP defined in [xx3].

By default, UPF and AS use tunnelling mode to exchange XRM traffic. The UPF and AS may use forwarded mode as defined in [xx3] when the XR flow is based on QUIC and they have negotiated Virtual ConnectionID via QUIC aware proxying with HTTP [xx3].

Upon the detection of uplink packet using PDR, UPF shall detect the QUIC flows to understand nature of QUIC flows. During UE and AS QUIC negotiation, UPF shall learn Connection IDs that are used in the flow from UE to AS and AS to UE. Based on learnt Connection ID, UPF may negotiate with AS per [xx3] to get Virtual ConnectionIDs. These virtual CIDs may be used by UPFand AS to support forwarding mode.

UPF and AS shall reuse same UDP 4-tuples.

When forwarding mode is active, UPF shall send QUIC packet received from UE over UPF-AS UDP 4-tuples in the uplink direction and Virtual ConnectionIDs negotiated via QUIC aware proxying with HTTP [xx3]. AS may send QUIC packet over UPF-AS UDP 4 tuples in the downlink direction and Virtual ConnectionIDs negotiated via QUIC aware proxying with HTTP [xx3].. The downlink packet shall use packet transformer [section 5.3 of XX3] to modify the content of QUIC packet.

During the negotiation between UPF and AS to activate the forwarding mode, UPF and AS shall agree to use specific packet transformer.

The downlink QUIC packets carrying XRM metadata has QUIC short header, XRM metadata and QUIC payload. XRM metadata is encoded into QUIC using packet transformer. UPF decodes QUIC using packet transformer to get XRM metadata and original QUIC packet.

.

*NEXT CHANGE (2)*

#### 5.8.5.3 Packet Detection Rule

The following table describes the Packet Detection Rule (PDR) containing information required to classify a packet arriving at the UPF. Every PDR is used to detect packets in a certain transmission direction, e.g. UL direction or DL direction.

**Table 5.8.5.3-1: Attributes within Packet Detection Rule**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Description** | **Comment** |
| N4 Session ID | Identifies the N4 session associated to this PDR. NOTE 5. |   |
| Rule ID | Unique identifier to identify this rule. |   |
| Precedence | Determines the order, in which the detection information of all rules is applied. |   |
| Packet  | Source interface | Contains the values "access side", "core side", "SMF", "N6-LAN", "5G VN internal". | Combination of UE IP address (together with Network instance, if necessary), CN tunnel info, |
| Detection | UE IP address  | One IPv4 address and/or one IPv6 prefix with prefix length (NOTE 3). | packet filter set, application identifier, Ethernet PDU Session |
| Information.NOTE 4. | Network instance (NOTE 1) | Identifies the Network instance associated with the incoming packet. | Information and QFI are used for traffic detection.Source interface identifies the |
|   | CN tunnel info | CN tunnel info on N3, N9 interfaces, i.e. F-TEID. | interface for incoming packets |
|   | Packet Filter Set | Details see clause 5.7.6. | where the PDR applies, e.g. from access side (i.e. up-link), |
|   | Application identifier |   | from core side (i.e. down-link), |
|   | QoS Flow ID | Contains the value of 5QI or non-standardized QFI. | from SMF, from N6-LAN (i.e. the |
|   | Ethernet PDU Session Information | Refers to all the (DL) Ethernet packets matching an Ethernet PDU session, as further described in clause 5.6.10.2 and in TS 29.244 [65]. | DN), or from "5G VN internal" (i.e. local switch). |
|   | Framed Route Information | Refers to Framed Routes defined in clause 5.6.14. | Details like all the combination possibilities on N3, N9 interfaces are left for stage 3 decision. |
|   | FQDN Filter for DNS Query | Contains one or more FQDN, FQDN range, and/or any FQDN. | The FQDN or FQDN range only used for detection of plain DNS Query message (i.e. not subject to ciphering). The usage is described in TS 23.548 [130]. |
|   | Protocol Description | Indicates service protocol used by the flow (NOTE 8) (NOTE 9) |   |
| Packet replication and detection carry on information | Packet replication skip information NOTE 7 | Contains UE address indication or N19/N6 indication. If the packet matches the packet replication skip information, i.e. source address of the packet is the UE address or the packet has been received on the interface in the packet replication skip information, the UP function neither creates a copy of the packet nor applies the corresponding processing (i.e. FAR, QER, URR). Otherwise the UPF performs a copy and applies the corresponding processing (i.e. FAR, QER, URR). |   |
| NOTE 6 | Carry on indication | Instructs the UP function to continue the packet detection process, i.e. lookup of the other PDRs. |   |
| Outer header removal | Instructs the UP function to remove one or more outer header(s) (e.g. IP+UDP+GTP, IP + possibly UDP, VLAN tag), from the incoming packet. | Any extension header shall be stored for this packet.  |
| Forwarding Action Rule ID (NOTE 2) | The Forwarding Action Rule ID identifies a forwarding action that has to be applied. |   |
| Multi-Access Rule ID (NOTE 2) | The Multi-Access Rule ID identifies an action to be applied for handling forwarding for a MA PDU Session. |   |
| List of Usage Reporting Rule ID(s) | Every Usage Reporting Rule ID identifies a measurement action that has to be applied. |   |
| List of QoS Enforcement Rule ID(s) | Every QoS Enforcement Rule ID identifies a QoS enforcement action that has to be applied. |   |
| NOTE 1:Needed e.g. if:-UPF supports multiple DNN with overlapping IP addresses;-UPF is connected to other UPF or AN node in different IP domains.-UPF "local switch", N6-based forwarding and N19 forwarding is used for different 5G LAN groups.-UPF "local switch" may be used for DNN/S-NSSAI dedicated for PIN.NOTE 2:Either a FAR ID or a MAR ID is included, not both.NOTE 3:The SMF may provide an indication asking the UPF to allocate one IPv4 address and/or IPv6 prefix. When asking to provide an IPv6 Prefix the SMF provides also an IPv6 prefix length.NOTE 4:When in the architecture defined in clause 5.34, a PDR is sent over N16a from SMF to I-SMF, the Packet Detection Information may indicate that CN tunnel info is to be locally determined. This is further defined in clause 5.34.6.NOTE 5:In the architecture defined in clause 5.34, the rules exchanged between I-SMF and SMF are not associated with a N4 Session ID but are associated with a N16a association.NOTE 6:Needed in the case of support for broadcast/multicast traffic forwarding using packet replication with SMF-provided PDRs and FARs as described in clause 5.8.2.13.3.2.NOTE 7:Needed in the case of packet replication with SMF-provided PDRs and FARs as described in clause 5.8.2.13.3.2, to prevent UPF from sending the broadcast/multicast packets back to the source UE or source N19/N6.NOTE 8:Not for PDR matching. It may be provided to assist PDU Set identification when PDU Set Identification and marking applies to the PDR and/or to assist identification of the last packet of the Data burst in downlink when End of Data Burst identification and marking in downlink applies to the PDR. See clause 5.8.2.4.2 and TS 26.522 [179].NOTE 9: In the case of encrypted XR media flow, PDU Set Identification and End of Data Burst information shall be available in the XRM metadata. If XRM metadata semantic is known in advance to UPF and AS, UPF shall not use this information. |

*NEXT CHANGE (3)*

#### 5.8.5.6 Forwarding Action Rule

The following table describes the Forwarding Action Rule (FAR) that defines how a packet shall be buffered, dropped or forwarded, including packet encapsulation/decapsulation and forwarding destination.

**Table 5.8.5.6-1: Attributes within Forwarding Action Rule**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Description** | **Comment** |
| N4 Session ID | Identifies the N4 session associated to this FAR. | NOTE 9. |
| Rule ID | Unique identifier to identify this information. |   |
| Action | Identifies the action to apply to the packet | Indicates whether the packet is to be forwarded, duplicated, dropped or buffered.When action indicates forwarding or duplicating, a number of additional attributes are included in the FAR.For buffering action, a Buffer Action Rule is also included and the action can also indicate that a notification of the first buffered and/or a notification of first discarded packet is requested (see clause 5.8.3.2).For drop action, a notification of the discarded packet may be requested (see clause 5.8.3.2). |
| Network instance(NOTE 2) | Identifies the Network instance associated with the outgoing packet (NOTE 1). | NOTE 8. |
| Destination interface(NOTE 3)(NOTE 7) | Contains the values "access side", "core side", "SMF", "N6-LAN", "5G VN internal". | Identifies the interface for outgoing packets towards the access side (i.e. down-link), the core side (i.e. up-link), the SMF, the N6-LAN (i.e. the DN), or to 5G VN internal (i.e. local switch). |
| Outer header creation(NOTE 3) | Instructs the UP function to add an outer header (e.g. IP+UDP+GTP, VLAN tag), IP + possibly UDP to the outgoing packet. | Contains the CN tunnel info, N6 tunnel info or AN tunnel info of peer entity (e.g. NG-RAN, another UPF, SMF, local access to a DN represented by a DNAI) (NOTE 8).Any extension header stored for this packet shall be added.The time stamps should be added in the GTP-U header if QoS Monitoring for packet delay is enabled for the traffic corresponding to the PDR(s). |
| Send end marker packet(s)(NOTE 2) | Instructs the UPF to construct end marker packet(s) and send them out as described in clause 5.8.1. | This parameter should be sent together with the "outer header creation" parameter of the new CN tunnel info. |
| Transport level marking(NOTE 3) | Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point. | NOTE 8. |
| Forwarding policy(NOTE 3) | Reference to a preconfigured traffic steering policy or http redirection (NOTE 4). | The Forwarding policy refers to a preconfigured forwarding behaviour in UPF, which may be related to:- N6-LAN steering to steer the subscriber's traffic to the appropriate N6 Service Functions deployed by the operator;- local N6 steering to enable traffic steering in the local access to the DN according to the routing information provided by an AF as described in clause 5.6.7;- a Redirect Destination and values for the forwarding behaviour (always, after measurement report (for termination action "redirect")). |
| Metadata(NOTE 10) | Metadata the UPF needs to add to traffic sent over a SFC. | The metadata information is associated with a TSP ID related to N6-LAN steering. |
| Request for Proxying in UPF | Indicates that the UPF shall perform ARP proxying and / or IPv6 Neighbour Solicitation Proxying as specified in clause 5.6.10.2. | Applies to the Ethernet PDU Session type. |
| Request for UDP Proxying in UPF | Indicates that the UPF shall perform QUIC tunnel towards AS as specified in clause 5.37.X.2 |  |
| Container for header enrichment(NOTE 2) | Contains information to be used by the UPF for header enrichment. | Only relevant for the uplink direction. |
| Buffering Action Rule(NOTE 5) | Reference to a Buffering Action Rule ID defining the buffering instructions to be applied by the UPF(NOTE 6) |   |
| NOTE 1:Needed e.g. if:-UPF supports multiple DNN with overlapping IP addresses;-UPF is connected to other UPF or NG-RAN node in different IP domains;-UPF "local switch" and N19 forwarding is used for different 5G LAN groups.NOTE 2:These attributes are required for FAR action set to forwarding.NOTE 3:These attributes are required for FAR action set to forwarding or duplicating.NOTE 4:The TSP ID is preconfigured in the SMF and used to determine the Forwarding Policy included in the FAR according to the description in clause 5.6.7 and clause 6.1.3.14 of TS 23.503 [45] for local N6 steering and in clause 5.6.16 and clause 6.1.3.14 of TS 23.503 [45] for N6-LAN steering. The Forwarding Policy action is enforced before the Outer header creation actions.NOTE 5:This attribute is present for FAR action set to buffering.NOTE 6:The buffering action rule is created by the SMF and associated with the FAR in order to apply a specific buffering behaviour for UL/DL packets requested to be buffered, as described in clause 5.8.3 and clause 5.2.4 of TS 29.244 [65].NOTE 7:The use of "5G VN internal" instructs the UPF to send the packet back for another round of ingress processing using the active PDRs pertaining to another N4 session of the same 5G VN group.NOTE 8:When in architectures defined in clause 5.34, a FAR is sent over N16a from SMF to I-SMF, the FAR sent by the SMF may indicate that the I-SMF is to locally determine the value of this attribute in order to build the N4 FAR rule sent to the actual UPF controlled by the I-SMF. This is further defined in clause 5.34.6.NOTE 9:In the architecture defined in clause 5.34, the rules exchanged between I-SMF and SMF are not associated with a N4 Session ID but are associated with a N16a association.NOTE 10:The use of Metadata is described in clause 5.6.16. How the UPF transforms the Metadata into actual information sent with the traffic (e.g. in the encapsulation header) is based on local policies related with the Forwarding Policy and not specified. |

*NEXT CHANGE (4)*

*NEXT CHANGE (5)*

*END OF CHANGES*