**3GPP TSG-SA2 Meeting #165**

**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:***  | Overview of the mechanisms defined 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 all mechanisms defined to support XRM metadata detection by UPF when XR traffic is encrypted between UE and AS |
|  |  |
| ***Consequences if not approved:*** | Not possible to support XRM metadata detection by UPF when XR traffic is encrypted between UE and AS  |
|  |  |
| ***Clauses affected:*** | 2 ; 5.37.1 ; 5.37.X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  |  |
| ***affected:*** |  | **x** |  Test specifications |  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

*FIRST CHANGE*

### 5.37.1 General

This clause provides an overview of 5GS functionalities for support of XR services (AR/VR applications) and interactive media services that require high data rate and low latency communication, e.g. cloud gaming and tactile/multi-modal communication services according to service requirements documented in TS 22.261 [2]. The standardized 5QI characteristics for such interactive services are provided in Table 5.7.4-1 and TSCAI is used to describe the related traffic characteristics as defined in clause 5.27.2. Further enhancements for these interactive media services are as follows:

- The 5GS may support QoS policy control for multi-modal traffic, see clause 5.37.2.

- The 5GS may support network information exposure which can be based on ECN markings for L4S, see clause 5.37.3 or 5GS exposure API, see clause 5.37.4.

- The 5GS may support PDU Set based QoS handling including PDU Set identification and marking, see clause 5.37.5.

- The 5GS may ensure that the UL and DL packets together meet the requested round trip delay and also update the delay for UL and DL considering QoS monitoring results, see clause 5.37.6.

- The 5GS may perform per-flow Packet Delay Variation (PDV) monitoring and policy control according to AF provided requirements, see clause 5.37.7.

- The 5GC may provide traffic assistance information to the NG-RAN to enable Connected mode DRX power saving, see clause 5.37.8.

- how The 5GC can handle end to end ciphered XR flows is defined in clause 5.37.X.

*NEXT CHANGE (2)*

### 5.37.X Handling of end-to-end encrypted XR flows

##### 5.37.X.1 General

This clause provides an overview of 5GS functionalities to support of XRM metadata detection by UPF when XR traffic is encrypted between UE and AS using QUIC protocol as defined in [166], SRTP with some RTP Header encryption [RFC 6904], or RTP Crytex [RFC 9335]. In those cases, the UPF can not read XRM metadata from RTP header extension fields.

The mechanisms defined in clause 5.37.X address only UE to XRM server (AS) communication and do not address UE-UE XRM communications. The mechanisms defined in clause 5.37.X address only downlink traffic handling.

The XRM metadata shall be encrypted and integrity protected between the UPF and the AS.

Three mechanisms are defined to carry XRM metadata between the UPF and the AS and further detailed in dedicated subclauses:.

* Use of Media over QUIC (MoQ) [xx1] ,
* Use of Proxy-UDP-in-HTTP/3 [xx2]+QUIC-Aware Proxying[XX3], and
* UDP-option [XX4]

For all these mechanisms once the UPF has retrieved clear text XRM metadata associated with a downlink PDU received over N6, the UPF can use these metadata to have proper QoS applied to this PDU, e.g. PDU Set based QoS marking towards the RAN, as defined in clause 5.37.5.

The 5GC (the UPF) determines which of the 3 mechanisms to apply to the traffic with a given AS based on configuration information e.g. received over the NEF.

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

##### 5.37.X.3 Usage of Media Over Quic in order to Handle end-to-end ciphered XR flows

##### 5.37.X.4 Usage of UDP options in order to Handle end-to-end ciphered XR flows

*NEXT CHANGE (3)*

# 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*.

[XX1] IETF draft-ietf-moq-transport: "Media over QUIC Transport".

[XX2] IETF RFC 9298: "Proxying UDP in HTTP".

[XX3] IETF draft-ietf-masque-quic-proxy-03: "QUIC-Aware Proxying Using HTTP".

[XX4] IETF RFC 9297: "HTTP Datagrams and the Capsule Protocol".

[XX5] IETF RFC 6904: "Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)".

[XX6] IETF RFC 9335: "Completely Encrypting RTP Header Extensions and Contributing Sources".

[XX7] IETF draft-ietf-avtcore-rtp-over-quic: "RTP over QUIC (RoQ)".

*NEXT CHANGE (4)*

*NEXT CHANGE (5)*

*END OF CHANGES*