**Agenda item:** **10.8**

**Source:** Lenovo

**Title: [FS\_5G\_RTP\_Ph2] End-to-end encryption scope and solutions space**

**Document for** Discussion andAgreement

# Introduction

This contribution discusses the scope of “end-to-end encryption” related to XR traffic in the context of FS\_5G\_RTP\_Ph2.

# Background

SA4 is discussing in KI#6 of FS\_5G\_RTP\_Ph2 [1] possible enhancements to PDU Set marking in case of XR end-to-end encrypted traffic. The topic stems out of SA2 FS\_XRM\_Ph2 SI [2] and its corresponding KI on:

“*WT#1.2 Support QoS control and PDU Set identification for XR stream with e2e encryption (e.g. fully encrypted header, partially encrypted header). This is applicable for PDUs received at N6 for DL.*”

So far, the KI#6 description was not documented in TR 26.822 of FS\_5G\_RTP\_Ph2 and no formal definition of “end-to-end encryption” has been provided in SA2 or SA4 for this matter, except the italic referenced text above from the FS\_XRM\_Ph2 SID [2].

# End-to-end Encryption of XR applications over RTP

The usage of encryption and in particular end-to-end encryption (e.g., IPSec tunneling, DTLS, HTTPS, QUIC) is broadly deployed nowadays across services, applications, and networks to provide security and privacy. In terms of the scope of this Key Issue, end-to-end encryption is the encryption of the application traffic (XR media) between a UE served in the 3GPP network and an application server in the cloud, or alternatively, another UE.

XR media delivery is highly user-centric and may include sensitive content pertaining to user FOV, screen content sharing, pose, movements, digital persona information, as well as metadata. It is expected that XR applications will employ encryption over-the-wire in some form to provide integrity and/or confidentiality of data in transit between remote endpoints.

WebRTC protocol stack (i.e., main delivery protocol for RTC in Rel-18 and currently in Rel-19) provides tools for secure transport of RTC media, i.e., SRTP for RTC media and DTLS for RTC data channel. Within the scope of FS\_5G\_RTP\_Ph2 only RTC media transport is being handled.

**Observation #1:** For PDU Set marking originating at the AS, the UPF generally requires access to the PDU Set marking information and the access in an end-to-end encryption context may imply some key exchange and decryption procedures when the PDU Set marking information is itself in ciphertext format.

**Observation #2:** For most XR applications it is already sufficient to ensure integrity-protection of RTP HE for PDU Set marking.

Based on the definition of “end-to-end encryption” (i.e., Proposal #1) and on Observation #1, the following categories of end-to-end encryption scenarios may be relevant in the context of KI#6 for FS\_5G\_RTP\_Ph2:

* Type I: Encrypted RTP SDU (incl. signed RTP HE for PDU Set marking)
	+ In this scenario the RTP payload is encrypted, but the RTP HE for PDU Set marking is available in plaintext over the wire (e.g., SRTP)
	+ The RTP HE for PDU Set marking may be however signed and integrity protected by means of SRTP strong authentication, i.e., the 80-bit authentication tag by RFC 3711.
	+ Pros:
		- RTP payload is confidentiality- and integrity-protected;
		- RTP PDU is integrity-protected;
		- RTP HE for PDU Set marking is integrity-protected and available in plaintext to the UPF;
		- Widely-deployed, well-tested and understood implementations of SRTP exist;
	+ Cons:
		- RTP HE for PDU Set marking is not confidentiality-protected and is available in plaintext to any middlebox/router in the path to N6;

NOTE 1: Type I end-to-end encryption scenario is supported by Solution #3.

* Type II: Encrypted RTP SDU + partly encrypted RTP header (incl. RTP HE for PDU Set marking)
	+ In this scenario the RTP payload is encrypted and a section of the RTP header is additionally encrypted (e.g., as RFC 6904 or as RFC 9335)
	+ The RTP HE for PDU Set marking is included in the RTP header section that is encrypted
	+ Pros:
		- RTP payload is confidentiality- and integrity-protected;
		- Additional RTP header metadata (e.g., CSRCs) and all or selected RTP HEs are confidentiality- and integrity-protected;
		- RTP HE PDU Set marking is in ciphertext and not available to access to any middlebox/router in the path to N6;
	+ Cons:
		- RTP HE for PDU Set marking is in ciphertext and PDU Set information is not available to access by the UPF;
		- Securing independently RTP HEs by RFC 6904 may experience some drawbacks such as:
			* Added complexity in key derivation and management as encryption context is done per RTP HE entity;
			* Only the RTP HE values are encrypted, but neither their lengths nor their identifiers which may leak privacy of RTP HEs in use;
			* The RTP HE identifier space may become bloated in case of legacy support of unencrypted RTP HEs, as both unencrypted and encrypted versions of an RTP HE need to be registered by SDP O/A procedures;
		- Encrypting CSRCs and RTP HEs as per RFC 9335 may still lack deployment maturity and support in practice as it has only been published in Jan. 2023;
* Type III: Encrypted RTP PDU
	+ In this scenario the RTP PDU is encrypted within an encrypted SDU of a secure envelope type of protocol, e.g., DTLS, QUIC, MoQ, RTP over QUIC (RoQ).
	+ Pros:
		- RTP PDU is confidentiality- and integrity-protected;
		- RTP HE PDU Set marking is in ciphertext and not available to access to any middlebox/router in the path to N6;
	+ Cons:
		- RTP HE for PDU Set marking is in ciphertext and PDU Set information is not available to access by the UPF;
		- Majority of solutions are at the transport-level, general and not media delivery specific (see NOTE 3 on MoQ) being out of scope of agreed SID of FS\_5G\_RTP\_Ph2 (see NOTE 4 on RTP over QUIC);
		- Generally, these solutions involve additional encapsulation overhead in comparison to Type I or Type II scenarios and solution space;
		- Such solutions may require additional infrastructure and/or protocol support on top of the core media delivery WebRTC-based protocol stack.

NOTE 3: MoQ has not been selected for Rel-19 packet-based media delivery as per approved FS\_AMD SID [3] and is out of scope of FS\_5G\_RTP\_Ph2.

NOTE 4: RTP over QUIC (RoQ) has been briefly discussed in Rel-18, but not formally documented. It is unclear what are the benefits that RoQ brings over SRTP, if any, besides end-to-end encryption of RTP header. Furthermore, an RTP profile over QUIC must handle and co-exist with QUIC significant and intricate mechanisms of flow and congestion control for which RTP has already many solutions tested and deployed over the years [4]. RoQ is still in draft stage in IETF, [5], and so it is not advisable to consider RoQ as a solution for end-to-end encryption in Rel-19 FS\_5G\_RTP\_Ph2.

**Observation #3:** Since some of the solutions within Type III scenario require further standardization efforts in other SDOs towards standardization completeness (e.g., MoQ, RoQ), it is advisable to not consider them in scope of FS\_5G\_RTP\_Ph2 for this Key Issue.

**Proposal #1:** It is advisable to document as part of KI#6 a formal definition of “end-to-end encryption” in the context of FS\_5G\_RTP\_Ph2.

**Proposal #2:** Rel-19 FS\_5G\_RTP\_Ph2 should focus on solutions space covering Type I and Type II end-to-end encryption scenarios.

# Conclusions

The following observations and proposals are derived based on the above description.

**Observation #1:** For PDU Set marking originating at the AS, the UPF generally requires access to the PDU Set marking information and the access in an end-to-end encryption context may imply some key exchange and decryption procedures when the PDU Set marking information is itself in ciphertext format.

**Observation #2:** For most XR applications it is already sufficient to ensure integrity-protection of RTP HE for PDU Set marking.

**Observation #3:** Since some of the solutions within Type III scenario require further standardization efforts in other SDOs towards standardization completeness (e.g., MoQ, RoQ), it is advisable to not consider them in scope of FS\_5G\_RTP\_Ph2 for this Key Issue.

**Proposal #1:** It is advisable to document as part of KI#6 a formal definition of “end-to-end encryption” in the context of FS\_5G\_RTP\_Ph2.

**Proposal #2:** Rel-19 FS\_5G\_RTP\_Ph2 should focus on solutions space covering Type I and Type II end-to-end encryption scenarios.

# 5 Proposal

The proposal is to discuss and agree on the contents of Clause 3 and proposed way forward summarized in Clause 4.

# References

[1] SP-240482, SID on 5G Real-time Transport Protocol Configurations, Phase 2, 3GPP SA Meeting #103, Mar. 2024.

[2] SP-231805, Revised SID on 5GS XRM Ph2, 3GPP SA Meeting #102, Dec, 2023

[3] SP-240478, SID on Advanced Media Delivery, 3GPP SA Meeting #103, Mar., 2024.

[4] M. Engelbert et. al, [Congestion Control for Real-time Media over QUIC (tkk.fi)](https://www.netlab.tkk.fi/~jo/papers/epiq21-rtp-over-quic.pdf), 2021.

[5] [IETF, draft-ietf-avtcore-rtp-over-quic-10: RTP over QUIC (RoQ) (ietf.org), Status: Experimental, expires 09 Nov. 2024.](https://www.ietf.org/archive/id/draft-ietf-avtcore-rtp-over-quic-10.html)