3GPP TSG-WG SA4 Meeting #127-bis-e S4-240769

Online, Apr 8 – 12, 2024 (revision of S4-240602)

**Source: Huawei, HiSilicon, Lenovo**

**Title: [FS\_5G\_RTP\_Ph2] Solution to key issue number #6 PDU Set marking for XR streams with RTP end-to-end encryption using SRTP**

**Document for: Discussion and approval**

**Agenda Item: 10.8**

**Work Item / Release: FS\_5G\_RTP\_Ph2 / Rel-19**

# 1. Introduction

The new SA4 Rel-19 study item on “5G Real-time Transport Protocol Configurations, Phase 2” (5G\_RTP\_PH2) has been approved in [SP-240065](https://www.3gpp.org/ftp/TSG_SA/TSG_SA/TSGS_103_Maastricht_2024-03/Docs/SP-240065.zip). The work item lists twelve distinct key issues to improve 5G RTP as defined in TS 26.522

1. ***PDU Set marking for XR streams with RTP end-to-end encryption.*** *This is an issue identified in SA2 XRM Phase 2 SI [3]. The current PDU Set identification relies on the RTP source to mark PDU Set with an RTP header extension defined in TS26.522. To support the case of end-to-end encryption, additional work may be needed in SA4.*

# 2. Proposal

The following is proposed to capture the following changes vs. TR 26.822.

\* \* \* \* First change \* \* \* \*

# 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*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[z0] IETF RFC 8285 (2017): "A General Mechanism for RTP Header Extensions", D. Singer, H. Desineni, R. Even.

[z1] IETF RFC 3711 The Secure Real-time Transport Protocol (SRTP)

 [z2] IETF RFC 9335 Completely Encrypting RTP Header Extensions and Contributing Sources

 [z4] 3GPP TS 26.522: "5G Real-time Media Transport Protocol Configurations".

[z5] IETF RFC 6904 (2013): “Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP), J. Lennox.

\* \* \* \* Second change \* \* \* \*(all new text)

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

HE (RTP) Header Extension

SRTP Secure RTP

\* \* \* \* Third change \* \* \* \*(all new text)

6.X Solution #X: SRTP Usage for end-to-end encryption

6.X.1 Key Issue mapping

Solution to key issue number #6 PDU Set marking for XR streams with RTP end-to-end encryption using SRTP

6.X.2 Description

When end-to-end encryption is applied, methods of inspecting the video bitstream will not work for PDU Set detection and NAL syntax cannot be read, neither.

Besides, when the RTP is tunneled over an end-to-end encrypted channel, the method of RTP header extension for PDU Set Marking in TS 26.522 [z4] will not work, neither.

As the RTP header extension (HE) for PDU Set marking uses the general mechanism for RTP Header Extensions from RFC 8285 [z0], it is not encrypted in secure RTP solution RFC 3711 [z1]. Therefore the SRTP could potentially be used together with RTP HE for PDU Set marking.

In Release 18 of TS 26.522 [z4] SRTP is supported, so this solution requires limited changes to TS 26.522 [z4] but some explicit text.

NOTE: Some cases when the RTP HE is also encrypted, e.g., RFC 6904 [z5], RFC 9335 [z2], are FFS.

\* \* \* \* End of changes \* \* \* \*