**3GPP TSG-SA4 Meeting #128 S4-241191**

***In revision of S4-240951***

**Jeju, South Korea, 20th – 24th May 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **Pesudo CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **26.822** | **CR** |  | **rev** |  | **Current version:** | **0.0.1** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | [FS\_5G\_RTP\_Ph2] Key Issue #6: PDU Set Marking for XR streams with RTP end-to-end encryption | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | FS\_5G\_RTP\_Ph2 | | | | |  | ***Date:*** | | | 2024-05-14 |
|  |  | | | |  | |  | | |  |
| ***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 can be 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | As agreed in SP-240482, a key issue for 5G\_RTP\_Ph2 was established to study applying and interpreting PDU set information. This change request documents the topics for study in the issue in the study TR 26.822 under development in SA4. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | TS 26.522 includes Header Extensions for marking PDU Set information in Release 18 and guidelines for interpreting PDU Set information in H.264/H.265 RTP streams.  As agreed in SP-240482, a key issue for 5G\_RTP\_Ph2 was established to study applying and interpreting PDU set information, considering the developments in the FS\_XRM\_Ph2 work in SA2 for end-to-end encryption cases. The issue is document as follows:  PDU Set marking for XR streams with RTP end-to-end encryption is one of the topics of the study 5G RTP phase 2.  Based on feedback received on S4aR240027 during the AhG call on Real Time Communication the following updates were completed to the proposed key issue description:.  1. The definition of end to end encryption was added  2. Mentioning of SA2 was removed as it is already mentioned in the note  3. No text was added about the support of web RTC data channel as it is assumed to be out of scope (as it is not RTP). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No clear key issue description, potentially no support for PDU Set identification in end-to-end encrypted setups | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.6.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Added confidentiality definition and merged against contribution S4-241095 | | | | | | | | |

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

## 5.6 Key Issue #6: PDU Set marking for RTP streams with end-to-end encryption

### 5.6.1 Description

Editor’s note: This clause provides a description of the key issue.

The usage of end-to-end encryption is broadly deployed in current networks to provide security. Similar security is expected for 5G RTP applications.

In this study, end-to-end encryption is referred to encryption that is commonly used in the industry that aims at the situation where only the two end users can access the confidential information but parties in between cannot.

Confidentiality is defined in this case as all user defined information being kept secret. This means that user related information from user A to user B is kept secret from other entities.

A 5G RTP end-to-end encrypted data flow contains RTP PDUs whose SDUs are encrypted, and headers may be partly encrypted.

Certain metadata not related to the information exchanged between the two parties need not be encrypted in this case. This follows industry best practices. For this issue the focus should be on the aspects within the scope of the study relating to XR media delivery.

This key issue proposes to study the enhancement of PDU Set Identification in encrypted RTP streams, in particular when using the RTP Header Extension for PDU Set marking.

The key issue should study the following aspects:

- Explore and document the different scenarios for providing end-to-end RTP encryption as targeted for 5G RTP

- If and how PDU Set information Identification may happen in an end-to-end encryption scenario for 5G RTP.

- If needed, develop methods for signalling PDU set Information for end-to-end encrypted RTP streams applicable to different methods of end-to-end encryption.

NOTE 1: Solutions that rely on breaking end-to-end encryption are out of the scope of this key issue.

NOTE 2: The work on this key issue may need coordination with SA WG2 and WG3.

NOTE 3: The end-to-end encryption based on QUIC is out of scope of this study

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