**3GPP TSG-SA3 Meeting #106-e *S3-220297-r1***

e-meeting, 14 - 25 February 2022 (revision of S3-yyxxxx)

**Source: Samsung**

**Title: New SID on 5G User plane security enhancements**

**Document for: Approval**

**Agenda Item: 4.18**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

# Title: Study on 5G User plane security enhancements

## Acronym: FS\_UPSec\_enh

## Unique identifier: *TBA*

## Potential target Release: Rel-18

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X | X | X |  |
| No |  |  |  |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | Work Task |
| X | Study Item |

## 2.2 Parent Work Item

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text}  |

Dependency on non-3GPP (draft) specification: N/A

# 3 Justification

Existing 3GPP User Plane (UP) security architecture and design has the following limitations:

1. **No support for selective protection of sensitive packets within a PDU session.** As UP security policy from the network is applied for the entire PDU session, granular activation or deactivation of security for a particular traffic within a PDU session is not supported. When activation of security is required for a particular traffic at PDCP layer, all traffic over that PDU session should be protected, which is an overhead, and may affect QoE for QoS sensitive traffic due to redundant cryptographic computations and may also lead to energy inefficiency. For example, considering the eXtended Reality (XR) applications in vertical industry, there are multiple types of traffic (different QCI) carried within a PDU session, such as streaming traffic (Real-time Media) and application layer signalling traffic (SIP/DNS messages). With the current technique, if the security is activated at PDCP layer for protection of application layer signalling traffic then streaming traffic is also protected at PDCP layer. There is no provision to deactivate protection of the streaming traffic at PDCP layer, even though it is protected at the application layer.

Application layer signalling traffic, e.g., (g)PTP (c.f., TS 33.501), DNS (c.f, TS 33.501), SIP (under discussion), ICMP (c.f., TS 33.501), requires protection at PDCP layer, which will enforce protection of all other traffic carried by the same PDU session.

The 5G verticals affected by the current design are (but not limited to), eXtended Reality (XR), Cloud Gaming and URLLC use cases. Also the 5G features affected are High-speed packetization and Energy Efficiency. To scale these applications and use cases appropriately, security need to be activated or deactivated with finer granularity (for example, up to a flow) and not for the whole PDU session.

1. **No support for isolation of UP keys between disaggregated CU-UPs.** Cryptographically separate UP keys are required between disaggregated CU-UPs i.e. when deployed at different locations. A compromise of an entity at a location may compromise the security in all other locations, if same key is used for a UE. Currently, CU-UPs deployed at different locations use the same UP security keys, which is serious security threat and, it is an important issue to be addressed. Even though SA3 initiated the study (FS\_disagg\_gNB\_Sec) in Rel-16 on this topic, due to lack of clarity on the scope of the SID and lack of consensus on the key issue, the study was closed (SP-200349). However, now there are disaggregated CU-UPs deployments foreseen, specifically in EDGE computing, Network slicing and URLLC use cases.

The 5G verticals affected by the current design are (but not limited to), EDGE computing, Network Slicing and URLLC use cases. Also the 5G features affected are: network slice enhancements and enhancements of Disaggregated gNB for 5G Advanced.

Considering the above limitations, there is a need to consider a security study in SA WG3 to enhance the UP security mechanism to support the emerging 5G vertical deployments and their requirements to enrich the system performance, while providing more flexibility without lowering the security level.

# 4 Objective

The objectives of this study are to:

1. Identify key issues and develop solutions to address the following UP security aspects:
	1. Support for selective protection of the UP data traffic within a PDU session, to enrich the system performance and energy efficiency.
	2. Support for disaggregated gNB architecture (where one UE connects to multiple gNB-CU-UPs) in 5GS without compromising the compartmentalization security requirements.
2. Conclude on selected solutions for potential normative work.

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 33.xxx | Study on 5G User plane security enhancements  | TSG#98  | TSG#99 | Rajadurai, Rajavelsamy, Samsung, rajvel@samsung.com |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A  | N/A  | N/A  |

# 6 Work item Rapporteur(s)

Rajadurai, Rajavelsamy, Samsung, rajvel@samsung.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential interactions with SA2 for the architectural aspects (security enforcement information), and RAN 2/3 for the RAN architectural aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Samsung |
| Deutsche Telekom |
| Interdigital |
| Lenovo |
| Motorola Mobility |
| CATT |
| Nokia |
| Nokia Shanghai Bell |
| NEC |
| Apple |
| ZTE |
| Motorola Solutions, Inc |
| Intel |
| Verizon |
| CableLabs |
| T-Mobile US |
| LG Electronics |