**3GPP TSG-SA3 Meeting #120 S3-25xxxx**

**Athens, Greece, 17 - 21 February 2025**

**Source: Samsung**

**Title: Pseudo-CR on IPsec ESP protocol**

**Document for: Approval**

**Agenda item: 5.20**

**Spec: 3GPP TR 33.938**

**Version: 0.1.0**

**Work Item: FS\_CryptoInv**

**Comments**

This contribution provides detailed description for IPsec ESP protocol used in 5G systems for TR 33.938.

\* \* \* First Change \* \* \* \*

### 4.4.x IPsec ESP

IPsec ESP is used in 5G system to provide security for the following:

Untrusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4]) and trusted non-3GPP access to the 5G core network (see clause 7 of TS 33.501 [4])

IP based interfaces for 5GC and 5G-AN according to NDS/IP (see clause 9 of TS 33.501 [4])

N2 interface between the AMF and the 5G-AN (see clause 9.2 of TS 33.501 [4])

N3 interface between the UPF and 5G-AN (see clause 9.3 of TS 33.501 [4])

Xn interface between 5G-AN (see clause 9.4 of TS 33.501 [4])

F1 and E1 of the gNB internal interfaces (see clause 9.8 of TS 33.501 [4])

Non-SBA interfaces internal to 5GC and between PLMNs (see clause 9.9 of TS 33.501 [4])

F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (see Annex M3.3 and M5 of TS 33.501 [4])

Policy discrimination of GTP-C, GTP-U and protection of GTP-C transport protocol (see Annex B of TS 33.210 [2])

Protection of IMS protocols and interfaces for all SIP signalling traversing inter-security domain boundaries. (see Annex C of TS 33.210 [2])

Protection of UTRAN/GERAN IP transport protocols and interfaces for all RANAP and RNSAP messages traversing inter-security domain boundaries. (see Annex D of TS 33.210 [2])

Security profile for IPsec ESP implementation in 3GPP are given in clause 5.3 of TS 33.210 [2].

IPSec ESP employs symmetric cryptography for confidentiality, integrity and replay protection.

\* \* \* End of Changes \* \* \* \*