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

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

**Source: Huawei, HiSilicon**

**Title: Pseudo-CR on IKEv2 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 IKEv2 protocol used in 5G systems for TR 33.938.

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

### 4.4.x IKEv2

IKEv2 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 clause M3.3 and M5 of TS 33.501 [4])

Security profiles for IKEv2 implementation and usage in 3GPP are given in clauses 5.2, 5.4, and 5.6 of TS 33.210 [2] and clauses 5, 6.2, and 7.5 of TS 33.310 [3].

IKEv2 employs symmetric cryptography for confidentiality and integrity protection.

IKEv2 employs asymmetric cryptography for digital signature and key agreement.

IKEv2 employs either symmetric cryptography or asymmetric cryptography for authentication.

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