**3GPP TSG-SA3 Meeting #101e S3-202977**

**e-meeting, 9 – 20 November 2020 Revision of S3-20xxxx**

**Source: Huawei, HiSilicon**

**Title: Threat analysis on no new created child SA**

**Document for: Approval**

**Agenda Item: 4.19**

# 1 Decision/action requested

***Approve this contribution to add a solution in TR33.520***

# 2 References

[1]

# 3 Rationale

Defined in TS 23.502, N3IWF shall determine the number of IPsec Child SAs to establish and the QoS profiles associated with each IPsec Child SA. For example, the N3IWF may decide to establish one IPsec Child SA and associate all QoS profiles with this IPsec Child SA. In this case, all QoS Flows of the PDU Session would be transferred over one IPsec Child SA. Therefore when a N3IWF cannot create a new child SA for different QoS, the user data will be sent in a channel that lead to a downgrade user experience or upgrade experience.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES \*\*\*

### Annex X (normative): Aspects specific to the network product class N3IWF

### X.Y No new created child SA

*- Threat name:* Create a new child SA for a PDU session

*- Threat Category*: Elevation of privilege.

*- Threat Description*: The N3IWF shall have the capaitlity to create a new child SA when a new QoS profiele is received. If when a new QoS profiles received which meets the trigger inside a N3IWF, but the N3IWF does not creat a new Child SA, the data of this PDU session maybe downgrade or upgrade by using a different QoS Channel. For example, if the new QoS profile is of much higher requirement than the existing QoS profiles, if the current Child SA could not support it, a new Child SA must be created, just to support the new QoS profile.  *- Threatened Asset*: Sufficient processing capacity.

\*\*\*END OF CHANGES\*\*\*