**3GPP TSG-SA3 Meeting #123 S3-2529944**

Goteborg, Sweden, 25 – 29 August 2025

**Source: China Mobile, Vodafone, Verizon, T-Mobile US, NTT DOCOMO, Telecom Italia, AT&T, BT, Charter Communications, Deutsche Telekom, IIT Bombay, KDDI**

**Title: pCR to TS 33.502 - Configuration requirements for Security related Events**

**Document for: Approval**

**Agenda Item: 5.1.1**

# 1 Decision/action requested

***Agree tdoc for incorporation into the draft TS 33.502***

# 2 References

[1] 3GPP TS 33.502 v0.0.1

# 3 Rationale

Based on approved WID (SP-250876), the working task needs to specify the general requirements for security events handling and collection.

In WT2, it will specify the events that need to be reported including the following.

- The NF collects information on the SBA layer about malformed messages it receives that deviate from the 3GPP specified messages or are considered invalid according to the protocol specification and network state.

- The NF collects information about events involving receiving a massive number of incoming messages on the SBA layer.

- The NF collects information about failed authentication and authorization attempts from inbound connections on the SBA layer.

- The NF collects information about potential replay attacks on the SBA layer.

- The NF collects information about potential abnormal SBI call flows as defined for the communication models in Annex E of TS 23.501.

It is proposed to add security requirements for configuration of security related events.

# 4 Detailed proposal

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

# 5 Requirements on Security related events

Editor’s Note: This clause addresses the general requirements to secure the procedures to configure, collect and delivery of security related events.

## 5.x Requirements on configuration for events detection and delivery

The 5G NF shall support the configuration capability for security related events based on operator’s decision.

The configuration capability shall support the type of security related events to be reported, the frequency of security events collection and frequency of reporting, the reporting type (e.g. push, on-demand, pull), the delivery destination, and activation/enablement of security events collection.

Editor’s Note: The detailed set of information elements to include for configuration is to be determined by SA5, and will be just referenced here.

The 5G system shall support mutual authentication between the 5GC NF (for configuration/activation of the functionality) and the Management Entity in charge of the configuration/activation of the events.

The 5G system shall support authorization to the Management Entity in charge of the configuration/activation of the events.

The 5G system shall support integrity protection, replay protection and confidentiality protection for communication between the 5GC NF and the Management Entity in charge of the configuration/activation of the events.

The 5G system should support the interaction between the 5GC NF and the Management Entity in charge of the configuration/activation of the events so that this interaction can be separated from other traffic including 5G management traffic.

Editor’s Note: Whether additional requirements are needed is FFS.

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