**3GPP TSG-SA3 Meeting #123 S3-252548**

Goteborg, Sweden, 25 – 29 August 2025

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

**Title: Security related Events Handling Overview**

**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

An overview of the architectural aspects for handling of Security related events is proposed. The proposal is based on agreed principles from TR 33.794 v19.1.0.

# 4 Detailed proposal

# \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*FIRST CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# X Overview of Security related Events Handling

The Service Based Architecture (SBA) is the dominant method for both control plane and management communications. In addition to the many benefits of using SBA, e.g. agility to increase and decrease the number of service instances in coordination with demand, an expanded attack surface appears for network, service and/or API security risks.

The 5G system includes heterogeneous and varied Network Functions (NF) deployments, where each and every Network Function has a specified behaviour according to 3GPP specifications. If any NF runs into errors, e.g. a violation of the normal behaviour, or abnormal access or unauthorised request, then the NF needs to be evaluated from security perspective. Collection of data related to abnormal events needs to be performed for the evaluation of the NF behaviour, with related data being transmitted towards a security entity that will execute the evaluation.

The following figure shows an example of trust domains in the overall architecture for the collection and transmission of the Security related Events detected by NFs.



Figure X-1 Example of trust domains in the Security related Events Handling architecture

NOTE 1: The definition of the trust domains is to be established by the PLMN-operator.

NOTE 2: The Security related Events Collecting entity is under operator control (e.g. through business agreements, policy, managed service, directly managed, etc) and it is out of the scope of 3GPP.

NOTE 3: The interface between the NFs and the Security related Events Collecting Entity is inside the scope of 3GPP.

NOTE 4: The interface between the Management Entity and the Security related Events Collecting Entity is not defined in this present document.

NOTE 5: Whether the security collecting entity is the same as the management entity is an operator decision.