**3GPP TSG-SA3 Meeting #124 S3-253789**

**Wuhan, China, 14 – 18 October 2025 merger of 519, 564 and 579**

**Source: China Mobile, Vodafone, AT&T, T-Mobile US, Verizon, Charter Communication, KDDI, Teliacom Italia, China Telecom, Ericsson?, Huawei?**

**Title: revision of example of trust domain**

**Document for: Approval**

**Agenda item: 5.1.1**

**Spec: 3GPP TS 33.502**

**Version: 0.1.0**

**Work Item: SECHAND**

**Comments**

It was commented in August meeting that trust domain figure is not fit for vendor’s real deployment. It proposes to revise the figure that tries to address the comment.

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

4 Overview of Security related Events handling

Editor’s Note: This clause addresses the architectural view of the feature

The Service Based Architecture (SBA) is the dominant method for control plane as well as the Service Based Management Architecture (SBMA) is for 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, potential attacks may still appear for network, service and/or APIs.

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 a 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.

\*\*\*following figure is new figure\*\*\*



**Figure 4-1 Example of trust domains in the Security related Events Handling architecture**

Editor’s Note: this figure is for information purposes to illustrate the requirement work. It will be revisited further once the requirements get agreed.

The NF gets configuration of security related events from the Management entity and delivers security related events through the Event transmitter. The Event transmitter could be an independent function or part of the NF. The Event transmitter is recommended to be part of an NF in order to reduce the attack surface. Whether the Event transmitter is inside the NF, outside the NF and inside the 5GC, or outside the 5GC, as depicted in Figure 4-1, is based on operator implementation.

The Event transmitter, Management Entity and Security related event collecting Entity are the end points of the related configuration and collection interfaces.The interfaces for collection of security related events are in scope of the present document. Requirements on the configuration of security related events are in scope of the present document. The interfaces between the Event transmitter and the NFs are out of the scope of 3GPP.

NOTE 1: Operators will define the relationship between trust zone

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

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