**3GPP TSG-SA3 Meeting #124 draft\_S3-253579-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: Ericsson**

**Title: Pseudo-CR on SECHAND architecture**

**Document for: Approval**

**Agenda item: 5.1.1**

**Spec: 3GPP TS 33.502**

**Version: 0.1.0**

**Work Item: SECHAND**

**Comments**

This contribution proposes an update of the example of trust domains in the overall architecture.

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

The security related event configuration entity configures the collection of security related events at the NF and/or optional event collection framework. The security related event collection entity collects security related events from the NF or optionally via an event collection framework. There is also management related event collection, but it is not in scope of this document. The optional event collection framework collects events from both 3GPP specified NFs and functions not specified by 3GPP, and potentially correlates different events, e.g. from different layers.

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.

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

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: Whether the security related event collection entity is the same as the security related event configuration entity is an operator decision. Communication between the security related event collection entity and the security related event configuration entity is not described in this document. Whether the security collection entity is the same as the management related event collection entity is an operator decision.

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