**3GPP TSG-SA3 Meeting #108-e draft\_S3-222064-r4**

**e-meeting, 22nd – 26th August, 2022 merger of S3-221791, S3-221781, S3-221920, S3-222064**

**Source:**  **Huawei, HiSilicon, Philips, Interdigital**

**Title:** **Add threat and requirement to key issue #1**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is proposed to approve the change described in this document.***

# 2 References

None

# 3 Rationale

5GS supports the policy and QoS differentiation for the traffic between a PINE and 5GS. The malicious, unauthenticated, and unauthorized PINE may use resources from 5GS. It’s proposed to add related threats and requirements.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

## 5.1 Key Issue #1: Authentication and authorization for PINE

### 5.1.1 Key issue details

A key aspect of the planned support of the 5G system for PIN is the ability of a UE (referred to as PEGC) to act as a gateway for PIN elements (PINEs), which are not acting as 5G UEs, to connect to 5GC.

According to TR 23.700-88 [2], a PINE without 3GPP capability cannot directly connect to the 5GC, but through the PEGC. Whether the PINE without 3GPP capability needs to be known by the 5GC and how to identify the PINE needs to be studied, e.g., for controlling access of the PINE to connecting 5G data networks, differentiating the PINE for policy provisioning, authorizing the PINE for traffic relay, etc.

### 5.1.2 Security threats

5GS supports the policy and QoS differentiation for the traffic between a PINE and 5GS. The network resource may be misused by the malicious, unauthenticated, and unauthorized PINE.

### 5.1.3 Potential security requirements

The PINE in a Personal IoT network should be authenticated.

The PINE in a Personal IoT network should be authorized.

**NOTE: further requirements might be added if found.**

\*\*\* END OF 1st CHANGE\*\*\*