**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250123-r1**

Online, Electronic meeting, 13 -16 January 2025

**Source: Philips International B.V.**

**Title: KI#3 update: Addressing ENs**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***SA3 is kindly requested to approve the following contribution.***

# 2 References

# 3 Rationale

*Regarding* Editor’s Note: It is FFS how the above threat affects various use cases

*Different use cases (including when using the same service e.g., inventory) may have different privacy requirements. It is therefore not possible to specify how the privacy threat affects the various use cases. It is sufficient for the privacy threat to be relevant for a subset of use cases to justify the need for addressing it. It is proposed to remove this Editor’s note.*

*Regarding* Editor’s Note: Security threat and requirement for potential exposure of quantity of devices after adversary broadcasts an inventory message is FFS

*It is proposed to remove this Editor’s Note as it is covered by KI#6.*

# 4 Detailed proposal

\*\*\* START OF CHANGES \*\*\*

## 5.3 Key issue #3: Privacy by protecting AIoT device identifiers

### 5.3.1 Key issue details

5G Ambient IoT service is a type of cellular IoT communication system where Ambient IoT devices utilize harvested energy to generate RF signals for bi-directional information transmission. Ambient IoT devices are characterized by limited functions, requiring only small and infrequent data transfers.

TS 22.369 [2] clause 5.2.6 defines the following privacy-related requirements:

“The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.”

In AIoT services, identifiers of AIoT device are used to identify the device. If the identifiers associated with a device are not privacy protected (e.g., exposed over the air), an attacker (e.g., an over-the-air attacker) can identify and track an AIoT device based on the identifiers associated with the AIoT device. Thus, this key issue is to investigate potential mechanisms to privacy protect the AIoT device identifiers.

### 5.3.2 Security Threats

An attacker can identify, monitor and track an AIoT device based on the identifiers associated with the AIoT device if the identifiers are not privacy protected.

### 5.3.3 Potential security requirements

Mechanisms for mitigating privacy threats (described above) by identifying, linking, and tracking the identifiers of AIoT Device(s) shall be supported.

Editor’s Note: AIoT use cases that do not need the above privacy protection mechanisms are FFS.

\*\*\* END OF CHANGES \*\*\*