**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250124-r1**

Online, Electronic meeting, 13 -16 January 2025

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

**Title: KI#4 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: Whether information protection can be done on application layer is ffs.

*It is proposed to remove Editor’s Notes under the following conditions:*

* *The Editor’s Notes are discussed and addressed in the conclusions.*

# 4 Detailed proposal

## 5.4 Key issue #4: Protection of information during AIoT service communication

### 5.4.1 Key issue details

As per TS 22.369 [2], Ambient power-enabled IoT (AIoT) services aim to support various use cases, including inventory taking, sensor data collection, asset tracking, and actuator control. These services intended to operate with lower power consumption and complexity than the existing IoT technologies such as eMTC, NB-IoT, and RedCap. To fulfil these requirements, AIoT devices require a communication capability.

Considering the ambient IoT device will be deployed in the indoor system, if the restricted access means (e.g., in factory) are provided, the possibility of attack is minimal. However, if the environment (e.g., in shopping mall) is open to the attacker, from a security perspective, security mechanisms to protect the information transmitted during AIoT service communication need to be supported. Failure to provide such security mechanisms will lead to various attacks such as eavesdropping, manipulation and/or unauthorized transmission of the information during AIoT service communication.

### 5.4.2 Security threats

For command operation (e.g., write, read), the following threats are applicable:

An attacker may acquire data transmitted to/from AIoT devices by eavesdropping messages if the communication of AIoT service is not confidentiality protected.

An attacker may manipulate information during communication of AIoT service if the communication of AIoT service is not integrity protected.

An attacker may replay a message if replay protection is not activated.

### 5.4.3 Potential security requirements

The Ambient IoT system shall support a means to ensure confidentiality, integrity and/or anti-replay of information for AIoT services.

Editor’s Note: Whether information protection between AIoT device and 5G core is mandatory is ffs.