**3GPP TSG-SA3 Meeting #116 *draft\_S3-242150-r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: Qualcomm Incorporated**

**Title: New Key Issue on the protection of information during AIoT service communication**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This contribution proposes a new Key issue in TR 33.713.***

# 2 References

[1] Draft TR 33.713 v0.1.0

# 3 Rationale

This contribution proposes a new Key Issue on the protection of information during Ambient power-enabled IoT (AIoT) service communication.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [1].

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

## 5.Y Key issue #Y: Protection of information during AIoT service communication

### 5.Y.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 that aligns with the characteristics of energy harvesting, low device complexity, low data rates, and long life span.

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.

Therefore, this key issue focuses on how to protect the information during AIoT service communication considering the specific use cases and limited device capability that are differentiated from the exiting IoT technologies.

### 5.Y.2 Security threats

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

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

### 5.Y.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 to which such protections are applicable.

Editor’s Note: Which entity (e.g. application function or core network entity) for information protection in the network side is FFS. Potential security requirements need to be aligned with the system architecture, service use cases and device capability which will be defined by other working groups.

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