**3GPP TSG-SA3 Meeting #115-AdHoc-e *draft\_S3-241435-r4***

e-meeting, 15th - 19th April 2024 merger of S3-241297, S3-241304, S3-241372, S3-241373, and S3-241400, S3‑241354

**Source: Qualcomm Incorporated, Huawei, HiSilicon, China Unicom, China Telecom, OPPO, InterDigital, CATT, Ericsson (?), Apple (?)**

**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] S3-24XXXX draft skeleton for AIoT security TR

[2] 3GPP TS 22.369: "Service Requirements for ambient power-enabled IoT"

# 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 are intended to operate with lower power consumption and cost than the existing IoT technologies such as eMTC, NB-IoT, and RedCap. To fulfill 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 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 existing 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 the communication of AIoT service if the communication of AIoT service is not integrity or replay protected.

### 5.Y.3 Potential security requirements

The 3GPP System shall support a means to ensure confidentiality, integrity, and anti-replay of information for AIoT services to which such protections are applicable.

Editor’s Note: whether the features to solve the above requirement are mandated or optional is FFS.

Editor’s Note: potential security solutions need to be aligned with the system architecture, service use cases, and device capability which will be defined by other working groups.

Editor’s Note: the additional requirements are FFS.

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