**3GPP TSG-SA3 Meeting #115-AdHoc-e *draft\_S3-241435-r1***

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

**Source: Qualcomm Incorporated, Huawei, HiSilicon, China Unicom, China Telecom, OPPO, InterDigital, 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 intended to operate with lower power consumption and cost 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 3GPP System shall support a means to ensure confidentiality, integrity or anti-replay of information for AIoT services to which such protections are applicable.

NOTE: Not all AIOT services/device types are expected to require support of features to solve the above requirement and hence support of such features are not mandated.

Editor’s Note: potential security requirements need to be aligned with the system architecture, service use cases and device capability which will be defined by SA2 and RAN2.

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