**3GPP TSG-SA3 Meeting #115-AdHoc-e *draft\_S3-241435-r6***

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, Nokia and Lenovo**

**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 \*\*\*\*\***

## X General Security Requirements

### X.Y Communication security requirements

The 3GPP 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: Applicability of the above security requirements in relation to AIoT services/device types 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 \*\*\*\*\***