**3GPP TSG-SA3 Meeting #117 *S3-24xxx***

**Maastricht, Netherlands 19 - 23 August 2024**

**Source: Huawei, HiSilicon**

**Title: New Key Issue for Authentication in Ambient IoT service**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the pCR to TR 33.713*[1]**

# 2 References

[1] 3GPP TR 33.713: "Study on Security Aspects of Ambient IoT Services in 5G".

# 3 Rationale

This contribution proposes a new key issue for TR 33.713 [1].

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 5.X Key Issue #X: Authentication in Ambient IoT service

### 5.X.1 Key issue details

The TR 23.700-13 [4] studies the architecture support of Ambient Internet of Things (AIoT) device, considering the service requirements for ambient power-enabled IoT device. In TR 23.700-13 [4], the validation of the AIoT device identity and authentication are explicitly mentioned.

### 5.X.2 Threats

In the air interface, an attacker may impersonate the victim device and report fake identification to the network side. If the network is not able to validate the reported identifier, the result exposed to the service consumer (e.g., AF) will be impacted. For example, in the use case of inventory taking as specified in TS 22.369 [2], the main purpose is to discover what goods (e.g., boxes, containers, packages, tools) are present in a specific area. If the fake identifications are collected, the inventory result will be not reliable. In addition, an attacker may send fake command request to the Ambient IoT devices. If the devices are not able to verify the command in the request message, devices will follow the fake command.

### 5.X.3 Potential security requirements

The 5G system should provide a means to perform authentication between the AIoT device and the network.

NOTE: each solution addressing this key issue needs to claim the entity (e.g., application function or core network entity) for authentication.

\*\*\* END OF CHANGE \*\*\*