**3GPP TSG-SA3 Meeting #115AdHoc-e draft\_S3-241113-r15**

**Electronic meeting, online, 15 - 19 April 2024** *revision of S3-24yyyy*

**Source: vivo, Interdigital, ZTE, Ericsson, OPPO, CATT, Qualcomm, Xiaomi, Lenovo, Apple, Nokia, Nokia Shanghai Bell**

**Title: Key issue on privacy by protecting AIoT device identifiers**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the pCR on new key issue on privacy for AIoT services.***

# 2 References

# 3 Rationale

This contribution proposes a new key issue on the privacy for AIoT services.

# 4 Detailed proposals

#### \*\*\* BEGIN CHANGES \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-49: "Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3".

[xx] 3GPP TR 23.700-13: “Study on Architecture support of Ambient power-enabled Internet of Things”.

#### \*\*\* NEXT CHANGES \*\*\*

## 5.X Key issue #X: Privacy by protecting AIoT device identifiers

### 5.X.1 Key issue details

5G Ambient IoT service is a type of cellular IoT communication system where Ambient IoT devices utilize harvested energy to generate RF signals for bi-directional information transmission. Ambient IoT devices are characterized by limited functions, requiring only small and infrequent data transfers.

TS 22.369 [x] clause 5.2.6 defines the following privacy-related requirements:

“The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.”

In AIoT services, identifiers of AIoT device can be used to identify the device. If the identifiers associated with a device are not sent over an interface, especially over the air, in a privacy-preserving manner, an attacker (especially an over-the-air attacker) can identify and track an AIoT device based on the identifiers associated with the AIoT device. Thus, this key issue is to investigate potential mechanisms to ensure handling of AIoT device identifiers in a privacy-preserving manner. .

### 5.X.2 Security Threats

If identifiers associated with an AIoT device is sent over an interface, especially over the air, in a non-privacy preserving manner, an attacker can identify and track an AIoT device based on the identifiers associated with the AIoT device. In the case of sensor data collection and asset tracking, if the device is used in a human wearable, then the location of the person wearing the wearable can be tracked. In the case of inventory taking and asset tracking, the adversary can gain competitive business advantage if it can track the location of its business rival’s goods and assets.

Editor’s Note: security threat and requirement for potential exposure of quantity of devices after adversary broadcasts an inventory message is ffs.

### 5.X.3 Potential security requirements

The mechanisms for mitigating privacy attacks (e.g., trackability of the device) by linking identifiers of AIoT Device(s) shall be supported.

Editor’s note: AIoT use cases that do not need the above protection mechanisms are FFS.

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