**3GPP TSG-SA3 Meeting #115AdHoc-e draft\_S3-241113-r1**

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

**Source: vivo, Interdigital, ZTE, Ericsson, OPPO, CATT, Qualcomm, Xiaomi, Lenovo**

**Title: Key issue on privacy for AIoT services**

**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 for AIoT services

### 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 and without the need for batteries.

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 TR 23.700-13 [xx], the AIoT services and corresponding information transfer have been identified by key issue#3 as following:

*"the following need to be supported:*

*- Inventory.*

*- Command.*

*The key issue will study the following aspects:*

*- Study how to support information transfer for Ambient IoT services and related system functionality, including the information transfer for an Ambient IoT device and for a group of Ambient IoT Devices. "*

In order to access AIoT services, the network will request the device ID or group ID from the AIoT device to verify its identity. Device ID is a unique identifier provided by the device owner, and is exclusively used to identify the owner's devices and manage related information for the associated services.The Inventory service uses the device ID or group ID to track the presence of a AIoT device and to count the number of AIoT devices in a specific area.

The Command service utilizes the device ID to locate the AIoT device and deliver the specific service data to the AIoT devices.

Thus, this key issue is to investigate methods to protect the privacy of sensitive parameters (such as the quantity of devices derived from Inventory service, the unique device ID, group ID) as depicted above considering the specific use cases and limited device capability that are differentiated from the exiting IoT technologies such as eMTC, NB-IoT and RedCap.

### 5.X.2 Security Threats

For inventory service, an attacker could potentially count the quantity of devices and track changes in device numbers within an area by observing the differences in reported device IDs after broadcasting an inventory message. The adversary can gain competitive business advantage if it can track the location of its business rival’s goods and assets.

If device ID does not have privacy protection, it may lead the following privacy incidents: exposure of device identifier, unauthorised detection of AIoT’s presence in certain location, unintentional tracking of AIoT’s movement, unauthorised knowledge of AIoT’s activity patterns, etc. If the device is used in a human wearable, then the location of the person wearing the wearable can be tracked.

If the AIoT device identifiers are not protected, an attacker could respond to the system query by sending answers with random device identifiers, that are counted by the system as genuine responses, e.g. a warehouse wants to count all TVs on stock and additionally to the responses it gets from the genuine AIoT devices, an attack may send additionally responses with changing identifiers, leading to a miscalculation in the system and to operational problems later on when devices needs to be shipped but are not there in reality.

### 5.X.3 Potential security requirements

The 5GS shall support a mechanism to ensure the protection of the sensitive parameters (e.g. quantity of devices derived from Inventory service, the unique device ID, the group ID) for AIoT services.

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.

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