**3GPP TSG-SA WG2 Meeting #163** **S2-2406983**

**27 May - 31 May, 2024, Jeju, South Korea (Revision of S2-2406129)**

**Title: [Draft] LS on Clarification of requirements for Ambient IoT**

**Response to: -**

**Release:** **Rel-19**

Work Item: FS\_AmbientIoT

Source: Ericsson (will be SA2)

To: SA1, RAN1, SA3

Cc: RAN2

Contact Person: Peter Hedman

E-mail Address: peter (dot) hedman (at) ericsson (dot) com

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** -

# 1 Overall description

While progressing the study on Ambient IoT, SA2 discussed some of the SA1 requirements in TS 22.369 and SA2 would like to ask SA1 the following questions:

**Question 1:** Are requirements for support of an unalterable/permanent equipment identification, also valid for Ambient IoT devices that only send uplink messages when triggered by the network?

TS 22.369 includes the following requirement:

### *5.2.6 Security and privacy*

*The 5G system shall enable security protection suitable for Ambient IoT, without compromising overall 5G security protection.*

*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.*

SA2 discussed the requirements listed above and is seeking clarification whether "suitable for Ambient IoT" means that the second requirement does not necessarily apply to all classes of Ambient IoT devices that may be supported in Rel-19.

Rel-19 Ambient IoT work focuses on indoor inventory and command scenarios, e.g., support of inventory in a warehouse. SA2 is specifically discussing whether for inventory taking (as described in TS 22.639 clause 4.3) there is a need to ensure privacy of the AIoT device identifier.

One issue that has been raised is whether it is feasible for very low complexity AIoT devices to support privacy protection as that typically requires an AIoT device to update its non-volatile memory after having been deployed (e.g., to update core network assigned temporary IDs). There is no consensus in SA2 whether a very low complexity AIoT device will always be able to update its non-volatile memory in typical deployment scenarios depending on available energy. There are also different views in SA2 whether privacy protection is required for all inventory taking scenarios.

**Question 2: Do the requirements listed in clause 5.2.6 of TS 22.369 for privacy protection apply to all classes of Ambient IoT devices that need to be supported in Rel-19? If these requirements do not apply to all classes of Ambient IoT, does this imply that such devices would be restricted to certain deployment scenarios?**

**Question 3: Does command signaling, e.g. for sensor data collection or actuator control in TS 22369 clause 4.3, need to generally be security protected (integrity and confidentiality protection)?**

TS 22.369 includes the following requirements:

### *5.2.3 Management*

*The 5G network shall support suitable management mechanisms for an Ambient IoT device or a group of Ambient IoT devices.*

*The 5G system shall support a mechanism to:*

*- disable the capability to transmit RF signals for one or more Ambient IoT device that is / are currently able to transmit RF signals*

*- enable the capability to transmit RF signals for one or more Ambient IoT device that is / are currently disabled to transmit RF signals*

*Based on operator policy, the 5G system shall provide a suitable mechanism to permanently disable the capability of an Ambient IoT device or a group of Ambient IoT devices to transmit RF signals. Subject to operator policy and regulatory requirements, the 5G system shall support suitable mechanisms for the Ambient IoT device to move between one or more networks and countries.*

**Question 3**: The last sentence above is stated as part of same paragraph and after the requirement on permanent disabling of device(s). Would it be correct understanding that the requirement has nothing to do with the previous requirement on permanently disabling of device(s)? Or is the AIoT device movement indeed related to the requirements on disabling and enabling the capability to transmit RF signals, e.g. if the disable/enable is done by a serving network that is not the same as the home network, i.e. is disabling of devices dependent or not dependent to certain network locations?

SA2 would like to ask the following question to RAN1:

**Question 4:** Can SA2 assume that a very low complexity AIoT device will always be able to update its non-volatile memory in typical deployment scenarios, e.g., when receiving a new temporary ID from the core network?

SA2 would like to ask SA3 the following question:

**Question 5**: Based on the answers provided by SA1, does SA3 foresee any required changes to existing security mechanism(s) with regards to AIoT devices using 3GPP access?

# 2 Actions

**To SA1 and RAN1**

**ACTION:** SA2 kindly asks SA1, RAN1 and SA3 to answer the relevant above questions.

# 3 Date of next TSG SA WG SA2 meetings

SA2#164 2024-08-19 – 2024-08-23 Maastricht, NL

SA2#165 2024-10-14 – 2024-10-18 India