3GPP TSG-SA3 Meeting #123 draft\_S3-252944-r2

Goteborg, Sweden, 25 – 29 August 2025

**Source: Qualcomm Incorporated**

**Title: Privacy protection of device ID in group inventory**

**Document for: Approval**

**Agenda item: 4.1.1**

**Spec: 3GPP TS 33.369**

**Version: 0.2.0**

**Work Item: Ambient\_IOT\_Sec**

**Comments**

This contribution proposes a mechanism to protect AIoT device identifier privacy during Inventory with filtering information (i.e., group inventory). The proposed mechanism is based on the mechanism captured in the living document (S3-252326), and is aligned with the inventory procedure described in S3-252806. Also, this contribution addressed the following editor’s notes in the living document.

Editor’s Note: whether AIOTF or ADM computes and checks T-ID is FFS.

Editor’s Note: in case AIOTF computes T-ID, how the KAIoTF is derived in ADM and how AIOTF retrieves the KAIoTF is FFS. In case ADM computes T-ID, the impact of interaction between AIOTF and ADM and the analysis of load of ADM is FFS.

Editor’s Note: which input key (e.g., KAIoT or KAIoTF) to be used is FFS

The above Editor’s Notes are deleted as the updated procedure proposes to have AIOTF hold the KAIoTF and generate a list of RESAIOT’. The proposal is intended to reduce the signaling overhead between AIOTF and UDM. We note that if AIOTF does not have a valid KAIoT, the bootstrapping procedure is performed as proposed in S3-252807.

Editor’s Note: whether AIOTF can acquire device ID from ADM is FFS.

The above Editor’s Note is removed as the AIOTF can retrieve the list of target AIoT device IDs from the ADM if the AIOTF does not already have the list. This retrieval can be done in the same manner as step 11 of clause 6.2.2 of TS 23.369.

Editor’s Note: How to address paging all case (i.e. paging message does not contain filtering information) is FFS.

As described above, the AIOTF retrieves the list of all target AIoT device IDs from the ADM. Thus, it is proposed to remove the above Editor’s Note.

Editor’s Note: whether and how to address Replay attack (e.g., replay RANDAIOT\_n to track the same T-ID) or DoS attack (e.g., energy depletion in AIoT device) is FFS.

Since the AIoT system is deployed as SNPN and limited to indoor scenario, it is proposed to add a NOTE that tracking the T-ID by replaying inventory request is not addressed in this specification, and remove the above Editor’s Note.

Editor’s Note: the format of the configured filtering information is FFS.

Editor’s Note: issues related filtering information is FFS.

It is proposed to remove the above Editor’s Notes and add a NOTE describing the configured filtering information prevents the AIoT device from matching the received filtering information that could reveal its AIoT device ID. Since such restriction (e.g., limiting which bits of AIoT device ID is allowed for filtering information) depends on specific use cases of filtering information, the format of the configured filtering information is left to the application layer.

Editor’s Note: whether a random number from device is required is FFS

For group inventory, random number from device is not used unless there is a following command procedure. Thus, it is proposed to remove the above Editor’s Note.

Editor’s Note: Whether network can provide network assigned T-ID to the AIoT device in command procedure is FFS.

This contribution proposes to use a temporary ID generated based on the KAIoT. Hence, it is proposed to remove the above editor’s note.

Lastly, we defined the function FA for RESAIoT’ calculation. Defining the cryptographic algorithm to realize FA (e.g., HMAC-SHA-256) is not the purpose of this contribution and can be discussed separately.

**Proposed Changes**

\* \* \* \* First change \* \* \* \*

## 5.4.3 The AIoT device identifier protection for inventory with filtering information

For the protection of AIoT device permanent ID during the inventory procedure described in clause 5.2.2, the following change shall apply:

- In step 4, the AIoT device determines it needs to reply to the NG-RAN based on the received filtering information.

NOTE: The attacker may obtain a AIoT device ID by performing a bitwise enumeration in multiple paging messages. To mitigate the attack, the AIoT device need to be configured with filtering information to match by limiting which bits of AIoT device identifier is allowed for filtering information (guidance would be to limit to the leftmost n bits of the permanent device identifier, e.g., only allow filtering information for the leftmost 64 bits and not respond otherwise).

- In step 5 and 6, a device identification information is not included in the D2R message and Inventory Report message.

- In step 7, filtering information is used as a device identification information if the AIOTF received it in step 0.

NOTE: The AIOTF identifies the AIoT device by checking the received RESAIoT. Therefore, device identification information is not needed in the D2R and Inventory Report message.

NOTE: When inventory with filtering information is used, after receiving the D2R message, the ADM has to exhaustively derive XRESAIoTs with all the long-term keys (i.e., KAIoT) of the AIoT devices in the group that was paged for every RANDAIoT\_d received. The AIOTF then, need to check XRESAIoT with the received RESAIoT. Therefore, the size of the group should be chosen accordingly to reduce the energy consumption, inter NF interaction, and latency.

\* \* \* \* End of change \* \* \* \*