3GPP TSG-SA3 Meeting #123 draft\_S3-252945-r2

Goteborg, Sweden, 25 – 29 August 2025

**Source: Qualcomm Incorporated**

**Title: Privacy protection of device ID in individual 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 an updated individual inventory procedure (i.e., inventory with AIoT device identifier) that protects AIoT device identifier privacy.

Note that the proposed procedure is identical to the authentication procedure described in S3-252806 as the authentication procedure is based on the Inventory procedure and already considered the identity privacy in sending the Inventory request and constructing the RESAIOT.

Also note that the proposed ID privacy mechanism is based on the option A in the living document (S3-252326) with updates to address the editor’s notes.

The proposed updates address the following Editor’s Notes in the option A of the living document:

Editor’s Note: whether AIoTF or ADM computes T-ID is FFS.

Editor’s Note: whether AIoTF or ADM computes T-ID’ is FFS.

Editor’s Note: in case AIoTF computes T-ID, a key KAIoTF derived from KAIoT in ADM is used. How AIOTF retrieves the KAIoTF is FFS.

Editor’s Note: in case the T-ID is computed by the ADM, whether the cryptographic key is the long-term key KAIoT or a key derived from KAIoT , and 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 temporary ID (i.e., T-ID) and RESAIOT that corresponds to T-ID’ in the Editor’s Note. 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 and how to address attacks of an attacker broadcasting T-ID and Nonce triggering all AIoT Devices to constantly compute T’-D (e.g., energy depletion in the AIoT devices) is FFS.

If an attacker constantly triggers Paging message with random T-ID and Nonce, the nearby AIoT devices would compute a T-ID and check if it is matched with the received T-ID for each Paging message. However, energy consumption of T-ID computation is not an issue because AIoT devices are assumed to harvest enough energy from RF signals for backscattering transmission. As long as the AIoT device can receive and decode Paging messages, the AIoT device should be able to perform T-ID computation. Therefore, it is proposed to remove the above Editor’s Note.

Editor’s Note: how to address the attack that manipulates the RANDAIOT\_N in the Paging message is FFS.

If an attacker manipulates the RANDAIOT\_N in the Paging message, the computed T-ID would not be matched with the received T-ID. Consequently, the AIoT device stops further processing of paging message as described in step 2. Therefore, it is impossible for an attacker to receive a valid Paging response from AIoT devices if the attacker manipulated the RANDAIOT\_N. In addition, the Paging message manipulated by the attacker does not affect subsequent Inventory procedure as AIoT devices do not maintain the received RANDAIOT\_N. Therefore, it is proposed to remove the above Editor’s Note.

Lastly, we defined the function FA for temporary ID derivation and 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 Protection of AIoT device identifier privacy

### 5.4.1 General

This clause describes the mechanisms to protect AIoT device identifier privacy during the inventory procedure. Depending on the situation and deployment scenario, the network operator can choose which paging procedure to use.

## 5.4.2 Procedure for AIoT Device identifier protection with Temp ID update during Individual inventory

#### 5.4.2.1 Individual Inventory Only Procedure

This procedure details how the Device Identity is protected when the network performs an Individual inventory only i.e. without a following command message.

The following high-level principles applies:

For Individual Inventory only, the network provides AIoT Device privacy by use of Temp ID in the paging message. The AIoT Device responds to the paging message with the Temp ID and integrity protection as described in clause 5.2.2. After completion of the Inventory procedure a new Temp ID is locally derived by both the AIoT Device and the network. The new Temp ID is used the next time the AIoT Device is individually paged.

Temp ID synchronization and re-synchronization are described in clause 5.4.2.3.



Figure: Option B.1 Procedure for Device ID protection during Individual inventory only

Procedure:

0. The AIoT Device has a pre-configured initial Temp ID\_0, the Network (the ADM) also have the initial Temp ID\_0 stored together with the device long term key, KAIOT in the AIoT Device profile.

1-3. Details of step 1-3 are specified in TS 23.369 [2]. No changes are needed to protect the AIoT Device Permanent ID.

NOTE 1: The Target Device Information provided by the AF addresses a specific device i.e., its AIoT Device Permanent ID.

4. The AIOTF requests the Temp ID\_n from the ADM. The ADM generate a RANDAIOT\_n as described in step 1 in clause 5.2.2 and fetches the current Temp ID\_n from the AIoT Device Profile. The ADM provides the Temp ID\_n and RANDAIOT\_n to the AIOTF.

5-6. Details of step 1-3 are specified in TS 23.369 [2]. No changes are needed to protect the AIoT Device Permanent ID.

7. The AIOTF sends an Inventory Request to the NG-RAN. The Inventory requests include Temp ID\_n, Correlation ID as specified TS 23.369 [2] and the RANDAIOT\_n. The Correlation ID is used to link response related this Inventory Request.

8. Details of this step is specified in TS 23.369 [2]. No changes are needed to protect the AIoT Device Permanent ID.

9. The NG-RAN Reader sends the paging message which includes the Temp ID\_n and the RANDAIOT\_n in the Container as specified in TS 38.300 [3]. The paging message shall indicate that it is a paging message that updates the Temp ID. If a AIoT Device matches its identity to the Temp ID\_n, the NG-RAN and AIoT device performs the Ambient IoT random access procedure as specified in TS 38.300 [3]. The AIoT Device generates a new Temp\_ID\_n+1 as specified in Annex X.Z and stores the new Temp ID\_n+1.

The AIoT Device sends the Inventory Response NAS message which includes the Temp ID\_n.

A failure case can happen when the AIoT device sends the inventory responds without being able to store the new Temp\_ID\_n+1 in its memory or an attacker manipulates the device to store a Temp\_ID\_n+1 when it should not have stored a new Temp\_ID\_n+1. The network can recover a AIoT device as specified in clause 5.4.2.3.

10. The NG-RAN forwards the NAS message to the AIOTF

11. The AIOTF request the ADM to verify the Inventory Response i.e., to check the authentication response form the device as specified in clause 5.2.2. The ADM reports the result of the message verification and optionally the AIoT Device Permanent ID. If the message was authentic. The ADM generates a new Temp ID\_n+1 in the same way as the AIoT Device did in step 9 and stores Temp ID\_n+1 it in the AIoT Device Profile.

12-14. Details of step 12-14 are specified in TS 23.369 [2]. No changes are needed to protect the AIoT Device Permanent ID

#### 5.4.2.2 Individual Inventory + Command Procedure

The following high-level principles applies:

When the Inventory + Command procedure is performed, the network generates a new Temp ID and send it securely to the AIoT device in the following Command message. It allows the AIoT Device to save some power of locally deriving a new Temp ID. The new Temp ID is used the next time the AIoT Device is individually paged.

Temp ID synchronization and re-synchronization are described in X.3.3.

This procedure details how the Device Identity is protected when the network performs an Individual inventory and when a command follows the inventory phase.



Figure: Option B.2 Procedure for Device ID protection during Individual + Command procedure

0. The AIoT Device has a pre-configured initial Temp ID\_0, the Network (the ADM) also have the initial Temp ID\_0 stored together with the device long term key, KAIOT in the AIoT Device profile.

1-6. Details of step 1-6 are specified in TS 23.369 [2]. No changes are needed to protect the AIoT Device Permanent ID.

7a-7b. AIOTF checks the Permanent ID with ADM. The ADM retrieves the stored Temp ID\_n and generate a session key and RANDAIOT\_n. ADM responds with the Temp ID\_n, the session key and RANDAIOT\_n that was used to derive the session key.

NOTE 1: The RANDAIOT\_n is used for authentication of the device as specified in clause 5.2.2. The Session key is used for command protection as specified in clause 5.3.2. Both parameters are included in this procedure for completeness, but not used for Device ID protection.

8. The AIoTF sends an Inventory Request to the NG-RAN. The Inventory requests include Temp ID\_n, Correlation ID, follow-on command indicator and RANDAIOT\_n. The Correlation ID is used to link all responses related this Inventory Request.

9. The NG-RAN sends an Inventory Response to the AIOTF with the Correlation ID indicating that the Inventory Request is received successfully and will perform the service operation accordingly.

10. The NG-RAN Reader sends the paging message which includes the Temp ID\_n, Command Indicator, and RANDAIOT\_n in the Container as specified in TS 38.300 [3]. The paging message shall indicate that it is a paging message that updates the Temp ID. If a AIoT Device matches its identity to the Temp ID\_n, the NG-RAN and AIoT device performs the Ambient IoT random access procedure as specified in TS 38.300 [3]. The AIoT Device derives the session key using the RANDAIOT\_n in the same way as ADM and includes the authentication Respone RESAIOT in the Inventory response message as specified in clause 5.2.2.

Editor’s Note: The Command Indicator may not be needed if an AS\_ID is assigned in msg2 by NG-RAN. This needs to be checked.

NOTE 2: An attacker that replay the paging message may trigger the AIoT device to start the RACH procedure again, but only until the AIoT device has received a new Temp\_ID\_n+1 in the following command message. In worst case the device will not have enough energy to handle the command message step 14-16.

The AIoT Device replies to the paging message with D2R with the Temp ID\_n.

11. The NG-RAN forwards the NAS message to the AIOTF in the Inventory Report message.

12. The AIOTF requests the ADM to verify the Inventory Response message and if verified to generate a new Temp ID\_n+1. The ADM generates a new Temp ID\_n+1 and responds to the AIOTF with the new Temp ID\_n+1.

NOTE: How the ADM generates the Temp ID\_n+1 is left for implementation.

13. AIOTF encrypts NAS message as specified in clause 5.3 using the session key, the NAS message includes both the command and new Temp ID\_n+1.

14. The NG-RAN Reader sends the R2D message which includes the encrypted NAS message (Command and new Temp ID\_n+1) in the Container as specified by RAN2.

15. AIoT device verifies and decrypts the NAS message and performs the command and stores the new Temp ID\_n+1.

A failure case can happen when the AIoT device sends the responds without being able to store the new Temp\_ID\_n+1 in its memory. The network can recover a AIoT device as specified in clause 5.4.2.3.

16. The AIoT Device send a D2R message that includes encrypted NAS message.

17. The NG-RAN sends a Command response that includes encrypted NAS message to the AIOTF. The AIOTF verifies and decrypts the NAS message. The AIOTF ask the ADM to store the Temp ID\_n+1in the AIoT Device Profile

18-19. Details of step 18-19 are specified in TS 23.369 [2].

#### 5.4.2.3 Out-of-Synch detection and Resynchronization of Temp\_ID

In case the network does not receive an Inventory Response from a AIoT Device after an Individual Inventory Request as described in 5.4.2.1 and 5.4.2.2, then it can indicate that the AIoT Device and network is out-of-synch with the Temp IDs. The out-of-synch can happen if e.g.,:

* The Inventory Response or Command Response from the Device was lost during transmission due to radio link issues e.g. interference, range, etc. in that case the AIoT Device would generate the Temp ID\_n+1, but the ADM would not generate the Temp ID\_n+1 or know that the device has received the Temp ID\_n+1 as it did not get any response.
* Something went wrong during the Inventory procedure e.g. the AIoT Device managed to write to the NVM but not send the inventory response or command response or the AIoT Device sent the inventory response or command response but was not able to write to the NVM.

This means that the ADM either has a Temp ID that is older or newer than the Temp ID in the AIoT Device. They can never be more than one off.

Temp ID sequence recovery is possible if the network performs Individual Inventory with both Temp ID\_n-1 or Temp ID\_n+1. When the AIoT device responds to the network, the network adjusts the sequence, and both are in synch again. Alternatively, the network can use the initial Temp\_ID\_0 to recover the device.

### 5.4.2a AIoT device identifier protection for inventory with AIoT device identifier

If Temp ID does not need to be updated, for the protection of AIoT device permanent identifier during the inventory procedure with AIoT device identifier described in clause 5.2.2, the following changes shall apply:

- In step 1, AIOTF shall retrieve a T-ID in addition to the RANDAIOT\_n from ADM. The ADM shall generate the T-ID using KAIoT, AIoT device permanent identifier and the RANDAIOT\_n as specified in Annex X.Z.

- In step 2, 3 and 4, the T-ID shall be used as a device identification information. The paging message shall indicate that it is a paging message that updates the Temp ID.

- In step 4, the AIoT device generates the T-ID in the same way as the ADM did in step 1. The AIoT device determines it needs to reply to the NG-RAN if the generated T-ID matches with the received T-ID.

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

- In step 7, the AIoT device permanent identifier is used as a device identification information.

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

\* \* \* \* Second change \* \* \* \*

# X.Z1 T-ID generation

When generating a temporary ID (i.e., T-ID) from KAIOT, the following parameters shall be used to form the input S to the KDF:

- FC = 0xCC,

- P0 = Temp\_n,

- L0 = length of Temp\_n,

- P1 = RANDAIOT\_n,

- L1 = length of RANDAIOT\_n

The input key KEY shall be KAIOT.

# X.Z2 Temporary Identity derivation function

When deriving a new temporary identity Temp ID\_n+1 from KAIOT, the following parameters shall be used to form the input S to the KDF:

- FC = 0xCC,

- P0 = RANDAIOT\_n,

- L0 = length of RANDAIOT\_n (i.e. 0x00 0x10),

- P1 = Temp ID\_n.

- L1 = length of Temp ID\_n (i.e. 0x00 0x10),

The input key KEY shall be KAIOT.

P1 input is either the stored Temp ID\_n when individual inventory procedure is executed or AIoT device Permanent ID when group inventory procedure is executed.

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