**3GPP TSG-SA3 Meeting #122 S3-25xxxx**

**Fukuoka, Japan, 19 - 23 May 2025**

**Source: Sony, Nokia?, Ericsson?, Oppo?, Huawei?, Lenovo?, ZTE?, Interdigital?, CATT?, others…**

**Title: KI#3, New Solution**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.8.0**

**Work Item: FS\_AIOT\_Sec**

**Comments**

Based on the discussion during the CC between SA3#121 and SA3#122 the following new merged solution is proposed.

**Proposed Changes**

\* \* \* First Change \* \* \* \*

## 6.xx Solution #XX: Temp ID protection for Ambient IoT device identifier

### 6.xx.1 Introduction

This solution addresses key issue #3 on privacy by protecting AIoT device identifiers. It is based on a temp ID generated by Ambient IoT device. Compared to the solutions with temp ID assigned by 5GC, this solution minimizes frequent sync-up procedures (writing operations) between 5GC and Ambient IoT Device by combining two methods of Temp ID generation based the use case when the AIoT Device is paged. The identified use cases are:

- Group Inventory, this can be stand-alone event or an event that precedes dedicated Command procedure as specified in TS 23.369.

- Individual Inventory only, this allows the network to check for one specific device

- Individual Inventory + Command, this allows the network to page one device and deliver a command to that device.

The details how the AIoT Device identities are protected are documented in the procedures. The following high level principles applies:

* For Group Inventory, no protection of the Target Device Information in the Inventory Request is added. It is assumed that e.g. the filtering information in the Target Device Information provides enough protection. Each AIoT Device that responds to the Inventory Request message will protect its identity by using a Temp ID derived using a freshness parameter in the inventory request. The network can verify the Temp ID and MAC in the inventory response.
* For Individual Inventory (both cases), the network adds protection to the Target Device Information (i.e., the Permanent ID) in the Inventory Request. The protection is based on the use of Temp ID in the Inventory Request message. The AIoT Device responds to the Inventory Request message with the Temp ID and MAC that the network can verify.
* The Device can match the Target Device Information or Temp ID directly without performing any calculation using the freshness parameter in the Inventory Request. Allowing the AIoT Device to spend minimum energy when parsing inventory requests not intended for the AIoT Device.
* Group Inventory with ALL, shall not be specified or allowed as such group inventory procedure will force the ADM to derive Temp IDs for all AIoT Device entries in the data base. The size of the group shall be considered.
* Temp ID synchronization and re-synchronization are described in separate clause 6.xx.2.4.

### 6.xx.2 Solution details

#### 6.xx.2.1 Group Inventory Procedure

This procedure details how the Device Identity is protected when the network performs a group inventory.



Figure 6.xx.2.1-1: Procedure for Device ID protection during group inventory

Procedure:

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

NOTE 1: The Target Device Information provided by the AF addresses a group of devices.

4. The AIOTF generate a NONCE\_nw. In this step the AIOTF may exchange the Target Device Information and NONCE\_nw with the ADM, but this can also be done in step 11.

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

7. The AIOTF sends a Inventory Request to the NG-RAN. The Inventory requests include Target device Information, Correlation ID as specified TS 23.369 and the NONCE\_nw. The Correlation ID is used to link all responses related this Inventory Request.

NOTE 2: The AIOTF does not add any protection to the Target device Information.

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

9. The NG-RAN Reader broadcasts the group Inventory Request which includes the Target device Information and the NONCE\_nw in the Container as specified by RAN2. If a AIoT Device matches its identify to the Target device Information it uses the NONCE\_nw to derive a Temp ID, NONCE\_d using an HMAC.



Figure 6.xx.2.1-2: Derivation of Temp ID and NONCE\_d

The NG-RAN and AIoT device performs the Ambient IoT random access procedure as specified by RAN2. The AIoT Device sends the Inventory Response NAS message which includes the Temp ID, NONCE\_d and MAC.



Figure 6.xx.2.1-3: Derivation of MAC

NOTE 3: The NONCE\_d and MAC is not needed for the AIoT Device ID protection, but used by the network to Authenticate the response message and protect against replay attacks

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

11. The AIOTF request the ADM to check the Temp ID(s) in the responses received linked to the Correlation ID. The ADM generates the Temp IDs of all AIoT Devices in the group of devices that matches to the Target device Information, in the same way as the AIoT Device did in step 9. The ADM reports the Permanent Device IDs to the AIOTF for each of the device that was verified during the check.

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

#### 6.xx.2.2 Individual Inventory Procedure

This procedure details how the Device Identity is protected when the network performs an Individual inventory.



Figure 6.xx.2.2-1: Procedure for Device ID protection during Individual inventory

Procedure:

The AIoT Device has a pre-configured Random number a.k.a. a SEED stored in the device. The Network (the ADM) also have the SEED stored together with the device Permanent ID, pre-shared key in the AIoT Device profile. Both the AIoT Device and ADM use the SEED to derive the Initial Temp ID\_0 and store it locally.



Figure 6.xx.2.2-2: Derivation of initial Temp ID

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

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

4. The AIOTF generate a NONCE\_nw. The AIOTF fetches the current Temp ID\_n from the Device Profile in the ADM or from local device context in the AIOTF.

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

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

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

9. The NG-RAN Reader sends the Individual Inventory Request which includes the Temp ID\_n and the NONCE\_nw in the Container as specified by RAN2. 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 by RAN2. The AIoT Device generates a new Temp\_ID\_n+1 and NONCE\_d and stores the new Temp ID\_n+1.



Figure 6.xx.2.2-3: Derivation of Temp ID\_n+1 and NONCE\_d

The AIoT Device sends the Inventory Response NAS message which includes the Temp ID\_n, NONCE\_d and MAC.



Figure 6.xx.2.2-4: Derivation of MAC

NOTE 3: The NONCE\_d and MAC is not needed for the AIoT Device ID protection, but used by the network to Authenticate the response message and protect against replay attacks

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

11. The AIOTF request the ADM to verify the Inventory Response by deriving the XMAC and check if the XMAC=MAC. The ADM reports the Permanent Device ID to the AIOTF if the message was authentic. The ADM generates the next Temp ID\_n+1 in the same way as the AIoT Device did in step 9 and stores Temp ID\_n+1.



Figure 6.xx.2.1-3: Derivation of XMAC

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

#### 6.xx.2.3 Individual Inventory + Command Procedure

After the Inventory procedure the AIOTF send a Command Request to the AIoT Device with the Temp ID stored in the ADM. In case the Command request was preceded by a group inventory the Temp ID =Temp ID\_n. In case the Command request was preceded by an Individual inventory the Temp\_ID=Temp ID\_n+1 generated and after completed inventory request procedure.

#### 6.xx.2.4 Temp\_ID Out-of-Synch detection and Resynchronization

In case the network does not receive an Inventory Response from a AIoT Device after an Individual Inventory Request as described in clause 6.xx.2.2, it can indicate that the AIoT Device and network is out-of-synch with the Temp IDs. This can happen if:

* The Inventory Response from the Device was lost during transmission due to radio 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 as it did not get any response.
* Something when wrong during the Inventory procedure e.g. the AIoT Device managed to write to the NVM but not send the inventory response or the AIoT Device sent the inventory 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 device responds to the network, the network adjusts the sequence, and both are in synch again.

The network can also verify the out-of-synch problem by performing a group inventory with a group that includes the specific device. If the device response to that group Inventory, the network knows that there is an out-of-synch issue. If the AIoT Device didn’t respond, the network knows that the device is not reachable and there may not be an out-of-synch issue.

An optional method to re-synchronize is to perform a group inventory with an indicator that indicates that the AIoT Device shall use the received NONCE\_nw as a new SEED and restart the Temp ID sequence using this SEED.

NOTE: All devices that receive and respond to the group inventory, will restart their Temp ID sequence. This optional method must be carefully used if specified.

### 6.xx.3 Evaluation

This hybrid solution has the following properties:

* Group Inventory will not require device to have an NVM or writing to the NVM. This will minimize the frequency of writes to the NVM as requested by RAN1.
* Individual Inventory will trigger the AIoT Device to write a new Temp ID to the NVM. That is aligned with RAN1 as they state that the device will be able to write at some point in time, meaning that the write may happen once enough energy has been harvested.
* A Temp\_ID is only used in one pair of messages (request + response).
* The Target Device Information in the group inventory is not protected by network layer security but assumed to be hard to parse if intercepted.
* There is no threat that the device Temp ID gets out-of-synch due to attacker broadcasting group inventory (e.g. replay of intercepted group inventory request). It will load the radio interface.

Editor’s Note: Further evaluation is FFS.

\* \* \* End of Changes \* \* \* \*