**3GPP TSG-SA3 Meeting #122 *S3-252326***

**Fukuoka, Japan, 19 – 23 May 2025 is revision of S3-25xxxx**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** | ***draft*** | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Living document for Procedure for Protection of AIoT device identifier privacy |
|  |  |
| ***Source to WG:*** | Sony, OPPO, Lenovo, Qualcomm Incorporated  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | AIOT\_Sec |  | ***Date:*** | 2025-05-23 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Living document for Procedure for Protection of AIoT device identifier privacy |
|  |  |
| ***Summary of change:*** | Adding Procedure for Protection of AIoT device identifier privacy |
|  |  |
| ***Consequences if not approved:*** | No support of the feature |
|  |  |
| ***Clauses affected:*** | 5.4 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

## 5.4 Protection of AIoT device identifier privacy

### 5.4.1 General

The protection of AIoT Device identifiers applies to the following use cases:

- Group Inventory, this can be stand-alone event or an event that precedes dedicated individual Command procedure as specified in TS 23.369 [2].

- Individual Inventory only, this allows the network to check for one specific AIoT Device.

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

The details how the AIoT Device identities are protected are documented in the procedures.

### 5.4.2 Procedures for AIoT Device identifier protection

#### 5.4.2.x Individual Inventory Procedure

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

Editor’s Note: It is FFS how to protect the AIoT Device ID when an individual AIoT Device is paged for an Individual Inventory that may or may not be followed by a command. The current situation is that there are two options (A and B) considered. These are captured in Annex X to document the status. More work is needed to reach consensus and complete the normative specification for this procedure.

#### 5.4.2.X Privacy protection of AIoT device ID in inventory with filtering information



Figure 5.4.2.X-1: Privacy protection of AIoT device ID in inventory with filtering information

1. Step 1-6 of clause 6.2.2 (Procedure for Inventory) or clause 6.2.3 (Procedure for command) of TS 23.369 [2] is performed. The AIoT\_Inventory request or the AIoT\_Command\_request contains the filtering information.

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

2. The AIOTF shall retrieve AIoT device IDs that match with the filtering information. Then, the AIoTF shall compute the list of T-IDs for the AIoT device IDs as specified in clause B.D.

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.

NOTE: Construction of the list can happen later, but before step 8.

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

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

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.

3. The AIoTF shall include the filtering information and RANDAIOT\_n in an Inventory Request and send the Inventory Request to the NG-RAN.

4. The NG-RAN shall send a Paging message containing the filtering information and RANDAIOT\_n.

5. Upon receiving the Inventory request, the AIoT device shall check if the filtering information matches with the configured filtering information. If they match, the AIoT device shall compute a T-ID as specified in clause B.D. If the filtering information does not match, the AIoT device shall stop further processing of the Inventory Request, i.e., the rest of the steps are not performed.

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

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

6. The AIoT device shall include the T-ID in an D2R message and send it to the NG-RAN.

7. The NG-RAN shall send an Inventory Report containing the T-ID to the AIOTF.

8. Upon receiving the Inventory response, the AIOTF shall find a matching T-ID. If there is a match, the AIOTF shall construct an AIoT\_Inventory Notify including the AIoT device ID that corresponds to the received T-ID.

9. The AIOTF continues with the procedures as specified in clause 6.2.2 or clause 6.2.3 of TS 23.369 [2].

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

\* \* \* Second Change \* \* \* \*

# B.D Temporary ID generation scheme

Temporary ID s are generated based the following parameters:

- AIoT device ID;

- RANDAIOT\_n;

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

Editor’s Note: which algorithm will be used for temp ID generation is FFS.

\* \* \* Third Change \* \* \* \*

# Annex X (Informative)

## X.1 Introduction

This annex is used to document two options (A and B) that are being considered as potential solutions to be specified in the normative clause 5.4. They are documented here to capture the progress made during several meetings. It must be noted that neither of the solutions in this annex have reached consensus to be normatively specified and further work on the solution may be needed. This Annex is to be deleted or voided once consensus have been reached.

The options in the following annex clauses address the following cases:

- Individual Inventory only, this allows the network to check for one specific AIoT Device.

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

## X.2 (Option A)

### X.2.1 Individual Inventory

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

The following high-level principles applies:

A temporary ID is generated and verified independently by the AIoT Device and network based on shared device credential and the NONCE included in the paging message. The AIoT Device does not store the temporary ID.



Figure X.2.1-1: Privacy protection of AIoT device ID in inventory with AIoT device ID

1. The AF initiates Inventory as specified in clause 6.2.2 of TS 23.369 [2]. The AIoT\_Inventory request contains the AIoT device ID.

2. The AIoTF shall obtain a T-ID, which is computed using a cryptographic key, the AIoT device ID and a randomly generated nonce, Noncenetwork as specified in clause X.2.1.B.D. Then, the AIoTF shall include the T-ID and Noncenetwork in an Inventory Request and send the Inventory Request to the NG-RAN.

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.

3. The NG-RAN shall send a Paging message containing the T-ID and Noncenetwork.

4. Upon receiving the Inventory request, the AIoT device shall compute a T-ID in the same way it was computed in the network X.2.1.B.D.

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.

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

If the computed T-ID does not match with the received T-ID, the AIoT device shall stop further processing of the Inventory Request, i.e., the rest of the steps are not performed.

 If the computed T-ID matches with the received T-ID, the AIoT device shall compute a T-ID’ using the same cryptographic key that the network used to compute T-ID, its AIoT device ID, the received Noncenetwork and a randomly generated nonce, Noncedevice as specified in clause X.2.1.B.E.

5. The AIoT device shall include the T-ID’ and Noncedevice in a D2R message and send it to the NG-RAN.

6. The NG-RAN shall send the Inventory Report containing the T-ID’ and Noncedevice to the AIoTF.

7. Upon receiving the Inventory response, the AIoTF shall obtain a T-ID’ as specified in clause X.2.1.B.E. If the computed T-ID’ matches with the received T-ID’, the AIoTF shall construct an AIoT\_Inventory Notify including the AIoT device ID that corresponds to the received T-ID’.

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

8. The AIoTF shall send the AIoT\_Inventory Notify to the AF as specified in clause 6.2.2 of TS 23.369 [2].

### X.2.1.B.D Temporary ID generation scheme 1

Temporary IDs are generated based on the following parameters:

- AIoT device ID;

- Noncenetwork;

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

Editor’s Note: which algorithm will be used is FFS

### X.2.1.B.E Temporary ID generation scheme 2

Temporary IDs are generated based on the following parameters:

- AIoT device ID;

- Noncenetwork;

- Noncedevice;

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

Editor’s Note: which algorithm will be used is FFS

## X.3 (Option B)

### X.3.1 Individual Inventory Only Procedure

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

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.x. 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.

Editor’s Note: How the integrity protection of the paging message as described in clause 5.x is FFS.

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



Figure X.3.1-1: Procedure for Device ID protection during Individual inventory only

Procedure:

0. The AIoT Device has a pre-configured initial Temp ID, the Network (the ADM) also have the initial Temp ID 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 generate a RANDAIOT\_n. The AIOTF fetches the current Temp ID\_n from the AIoT Device Profile in the ADM or from local device context in the AIOTF.

Editor’s Note: which entity (e.g., AIOTF or ADM) generates a RANDAIOT\_n is FFS.

Editor’s Note: how Temp ID\_n is generated, and which key is used is FFS.

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\_nin the Container as specified in TS 38.300 [3]. 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 and RANDAIOT\_d and stores the new Temp ID\_n+1.

Editor’s Note: how to handle if the AIoT device could not store the new Temp ID is FFS.

Editor’s Note: how and why RANDAIOT\_d is generated from RANDAIOT\_N is FFS.

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

Editor’s Note: how to address the attack that spoofs the D2R message is FFS. The D2R spoofing attack results into the incorrect inventory results in the network and introduces a de-synchronization of the Temp ID between the AIoT device and network.

NOTE 2: The RANDAIOT\_d is not used to protect the AIoT Device Identifier. It is used to provide integrity protection of the response as described in clause 5.2.

Editor’s Note: how the RANDAIOT\_d is used to provide the integrity protection of the response is FFS.

Editor’s Note: which algorithm will be used is FFS



Figure X.3.1-2: Derivation of Temp ID\_n+1 and RANDAIOT\_d

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

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

11. The AIOTF request the ADM to verify the Inventory Response. The ADM reports the result of the message verification and optionally the AIoT Device Permanent ID. 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 and stores it in the AIoT Device Profile.

NOTE 3: The message verification is specified in clause 5.2.

Editor’s note: The impact of interaction between AIOTF and ADM is FFS. The analysis of load of ADM is FFS.

Editor’s Note: how to ensure privacy if the same temp ID is used several times due to the loss of the messages, write failure, or attacks.

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

### X.3.2 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 X.3.2-1: 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.

Editor’s Note: how the session key is derived is FFS.

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]. 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 integrity protects the Inventory response message as specified in clause 5.2.

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.

Editor’s Note: Integrity protection of the Inventory response message is FFS.

Editor’s Note: How to address the replay attack is FFS.

Editor’s Note: Linkability between step 10a (Paging request) and step 10d (D2R message) is FFS.

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 verifies the Inventory Response message. The AIOTF requests the ADM to generate a new Temp ID\_n+1. The ADM generates the next Temp ID\_n+1 and stores it in the AIoT Device Profile.

Editor’s note: The impact of interaction between AIOTF and ADM is FFS. The analysis of load of ADM is FFS.

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.

Editor’s Note: how to handle if the AIoT device could not store the new Temp ID is FFS.

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.

Editor’s Note: how to ensure the privacy if the same temp ID is used several times due to the loss of the messages, write failure, or attacks.

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

## X.3.3 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 X.3 and X.4, it can indicate that the AIoT Device and network is out-of-synch with the Temp IDs. This 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 device responds to the network, the network adjusts the sequence, and both are in synch again.

The network can 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.

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