**3GPP TSG-SA3 Meeting #123 draft\_S3-252942**

**Goteborg, Sweden, 25 – 29 August 2025**

**Source: Xiaomi**

**Title: Addressing ENs in AIoT authentication procedure**

**Document for: Approval**

**Agenda item: 4.1.1**

**Spec: 3GPP TS 33.369**

**Version: 0.2.0**

**Work Item: AmbientIoT-SEC**

**Comments**

It is proposed to address the following ENs in the AIoT authentication procedure.

Editor’s Note: Whether ADM or AIOTF generates RANDAIOT\_n is FFS.

To reduce the interaction between the AIOTF and ADM, it is proposed that AIOTF generate RANDAIOT\_n for authentication. Otherwise, one additional round of messages is necessary for transmitting the RANDAIOT\_n, i.e. one message from the AIOTF to ADM for requesting the generation of RANDAIOT\_n, and one message from the ADM to AIOTF for providing the RANDAIOT\_n.

Editor’s Note: Whether replay attack is possible is FFS.

Editor’s Note: Whether RANDAIOT\_d is required for inventory procedure is FFS.

Since the Inventory request is not protected, the replay attack can always be launched. However, the device authentication is determined by verifying the RES, which is generated at least by using RANDAIOT\_n included in the Inventory request. If the verification of RES fails, the replay attack can be detected by the network side. Therefore, the attacker cannot manipulate the AIoT system by launching a replay attack during the inventory procedure.

During the authentication procedure, each peer entity should provide a random number to ensure freshness. Therefore, it is proposed to include RANDAIOT\_d in the inventory response and use it as one of the input parameters for generating the RES. With RANDAIOT\_d and RANDAIOT\_n, the security of authentication can be further enhanced.

Editor’s Note: How RESAIOT is derived and whether it is derived from KAIoT or intermediate key is FFS.

Editor’s note: The impact of interaction between AIOTF and ADM is FFS. If the authentication is expected to be run more often than normal UE, (e.g., during each inventory procedure), the analysis of load of ADM is FFS.

Considering the storage limitation of AIoT device, it is proposed that the KAIOTF is refreshed during each inventory + command procedure. In this case, the AIoT device do not need to store the security context, which can meet the requirement from RAN. The KAIOTF can be generated by the ADM from KAIOT and provided to the AIOTF to protect the command message. Regarding the load of ADM, it can be left to the implementation of the private network.

Considering the security functionality of AIOTF and ADM, and the primary authentication procedure in SNPN (clause I.2.2.2.2 of TS 33.501), it is proposed that ADM calculate XRES by using the KAIoT and determine the authentication result by verifying RES. Therefore, the security functionality of AIOT system will be:

* The ADM is responsible for the authentication and credential management.
* The AIOTF is responsible for the communication protection.

Editor’s note: How to perform the mutual authentication for command procedure will be specified.

To save the calculation resources and transmission resources of AIoT device, the implicit authentication method can be used for mutual authentication. By verifying the security of command request message, the AIoT device can implicitly determine the authentication result to the network.

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

### 5.2.2 Authentication procedure

The authentication procedure is aligned with inventory procedure and command procedure in 6.2.2 and 6.2.3 of TS 23.369[2].



Figure 5.2.1-1: Authentication procedure

0. Step 1-6 of clause 6.2.2 Procedure for Inventory or clause 6.2.3 Procedure for command in TS 23.369 [2] is performed.

1. ADM shall generate RANDAIOT\_n.

2. AIOTF shall send inventory request message including RANDAIOT\_n to NG-RAN.

3. NG-RAN shall send the paging request message including RANDAIOT\_n to the AIoT device.

4. Upon receiving the paging request message, AIoT device shall generate RN 16 and derive RESAIOT using KAIoT, RN 16 and RANDAIOT\_n for network authenticating AIoT Device.

NOTE: Use of the AIoT root key KAIoT for authentication assumes there is only one security domain in the present document.

NOTE: Device generated RAND during individual and group inventory procedure is RN 16. RN 16 could also be used for privacy protection purpose if needed. How to use RN 16 for privacy protection purpose is specified in 5.4.

Editor’s Note: Where the authentication credentials are processed in AIOT device is FFS.

5. AIoT device sends D2R message to the NG-RAN, including RESAIOT and RN 16 from device.

6. NG-RAN sends Inventory report message to AIOTF, including the RESAIOT and RN 16.

7. AIOTF sends device identifier and RN 16 to ADM.

8. ADM derives XRESAIOT using the same method as in AIoT device. For inventory and command case, ADM shall derive command protection key and send to AIOTF.

Editor’s Note: Where the authentication credential is processed in AIOT device is FFS.

9. ADM sends XRESAIOT to AIOTF.

10. AIOTF verifies RESAIOT. If the verification is successful, the steps 12-14 in clause 6.2.2 for inventory procedure or the step 8-11 of clause 6.2.3 for command procedure in TS 23.369 [2] continues.

For inventory and command case, the network is implicitly authenticated by the device via the successful verification of the MAC for command request integrity protection. MAC shall be derived using the integrity protection key and network generated random number included in the command request as in 5.3.3.

1. AIOTF shall construct a NAS Command Request including MAC and RANDAIOT\_n2 . AIOTF sends NAS Command Request to AIoT RAN Reader.
2. AIoT RAN Reader shall send NAS Command Request includes MAC and RANDAIOT\_n2 to AIoT Device.
3. AIoT Device receives NAS Command Request and shall decide mutual authentication is needed, and shall derive XMACas the same way as AIOTF. AIoT Device shall verify the MACAIOT to authenticate the network.

AIoT Device shall derive communication protection key KAIoTF in this step. The method of KAIoTF derivation is descried in 5.3.X.

1. AIoT device sends Command response to RAN Reader, indicating successfully authenticating network.
2. RAN Reader sends Command response to AIOTF.

Step 11-15 is aligned with clause 6.2.3 Procedure for Command in TS 23.369 [2].

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

Annex X (normative):
Key derivation functions

# X.1 RESAIOT and XRESAIOT derivation function

When deriving a RESAIOT and XRESAIOT from KAIOT, the following parameters shall be used to form the input S to the KDF:

- FC = 0x6B,

- P0 = RANDAIOT\_n,

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

- P1 = RN 16.

- L1 = length of RN 16 (i.e., 0x00 0x10),

The input key KEY shall be KAIOT.\* \* \* Third Change \* \* \* \*

### 5.3.3 Input parameters to integrity algorithm

The input parameters to the integrity algorithm as described in Annex D.3 in TS 33.501[5] shall be set as follows.

The KEY input is equal to the KAIOTF key. The fresh network generated random number is used to derive the KAIOTF key and the MAC.

Editor’s Note: whether the KAIOTF key is fresh for each round of inventory-command procedure is FFS.

The DIRECTION bit is set to 0 for uplink and 1 for downlink.

The BEARER is set to all zeros.

The COUNT is set to all zeros.

Editor’s Note: input key is FFS.

NOTE: This document assumes that for inventory and command case, only one subsequent command request after inventory.

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