**3GPP TSG-SA3 Meeting #124 draft\_S3-253677-r8**

Wuhan, China, 13 - 17 October 2025

**Merger of S3-253167, S3-253281, S3-253472~~,~~ S3-253504, S3-253505, S3-253472, S3-253531, S3-253251**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **017** | **rev** | 1 | **Current version:** | **0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Update of authentication procedure |
|  |  |
| ***Source to WG:*** | OPPO, CATT, InterDigital, Vivo, Huawei, HiSilicon, Lenovo, Ericsson, Qualcomm |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2025-09-22 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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:*** | Various terminology are not consistent and editor’s note remain. |
|  |  |
| ***Summary of change:*** | Fixed terminology alignment and removal of several editor’s notes. |
|  |  |
| ***Consequences if not approved:*** | Incoplete specification |
|  |  |
| ***Clauses affected:*** | 4.2.1.2, 5.2.1, 5.2.2 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*BEGIN OF CHANGES\*\*\*\*\*\*\*\*\*\*\*\*\*

4.2.1.2 Requirements related to authentication between device and network

The AIoT device shall support:

- a method for pseudo-random bit generation

\* \* \* Next Change \* \* \* \*

5.2 Authentication procedure

5.2.1 General

This clause describes the authentication procedure for Ambient IoT devices for both Inventory procedure and Command procedure when authentication is triggered by the network. Device authentication shall always be performed for the Inventory procedure.

NOTE: KAIOT\_root is the long-term key.

5.2.2 Authentication procedure

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



Figure 5.2.1-1: Authentication procedure

 0. Step 1-6 of Clause 6.2.2 for the inventory procedure or Clause 6.2.3 for the command procedure in TS 23.369 [2] is performed.

1. ADM shall generate RANDAIOT\_n. AIOTF shall retrieve RANDAIOT\_n from ADM.

2. AIOTF shall send Inventory Request message, including RANDAIOT\_n in addition to the AIoT Identification Information specified in clause 6.2.2 of TS 23.369 [2] to NG-RAN.

3. NG-RAN shall include RANDAIOT\_n in the paging message to the AIoT Device in addition to the AIoT Iidentification Iinformation.

 NOTE 1: An active attack may send a new paging message to the AIoT Device while there is an ongoing procedure in the AIoT Device. The AIoT Device will abort the ongoing procedure and respond to the new paging message. The security measure to such Denial-of-Service attack is not specified in present document.

NOTE 2: While a legitimate network is performing an inventory operation, an attacker may cause amplification of resource exhaustion at the legitimate network side by sending AIoT paging messages for all AIoT Devices or to a large group of AIoT Devices, which causes large number of AIoT Devices sending D2R messages to the legitimate network that the legitimate network does not expect to receive. The security measure to such amplification of resource exhaustion attack is not specified in present document.

4. Upon receiving the paging message, if the AIoT Device determines it needs to respond based on the AIoT Identification Information, the AIoT device shall generate a pseudo-random number RANDAIOT\_d, calculate RESAIOT using KAIoT\_root, RANDAIOT\_n, RAND\_AIOT\_d (see Annex A.2) for network authenticating AIoT Device.

Editor’s Note: the randomness of RANDAIOT\_d is FFS.

5. AIoT Device shall send a D2R message including an AIOT NAS message to the NG-RAN. The AIOT NAS message includes RESAIOT , and RANDAIOT\_d.

6. NG-RAN shall send an Inventory Report message to AIOTF, including the AIOT NAS message containing RESAIOT , and RANDAIOT\_d.

7. AIOTF shall send the AIoT Identification Information, RANDAIOT\_n and RANDAIOT\_d to ADM.

NOTE 3: The authentication is expected to be run more often than normal UE (i.e., during each inventory procedure), which has load impact to ADM.

8. ADM shall calculate XRESAIOT using the same method as in AIoT Device (see Annex A.2).

9. ADM shall send ~~the~~ XRESAIOT to AIOTF.

10. AIOTF shall verify RESAIOT. If the verification is successful, for command case, the AIOTF shall retrieve KAIoTF from ADM. ADM shall calculate KAIoTF if it receives a request from AIOTF (see AnnexA.3).

The steps 12-14 in clause 6.2.2 for inventory procedure or the step 8-11of clause 6.2.3 for command procedure in TS 23.369 [2] continue.

For the command procedure, the AIoT device implicitly authenticates the network via integrity check of the AIOT NAS Command Request message as specified in clause 5.3.2 of present document.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* CHANGES END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***