**SA WG2 Meeting #170S2-250xxxx**

**25 - 29 August, 2025, Goteborg, Sweden (revision of S2-25xxxxx)**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **23.369** | **CR** | **xxxx** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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 |  | Radio Access Network | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Resolve Security Related ENs in AIoT Procedure |
|  |  |
| ***Source to WG:*** | ZTE  |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | AmbientIoT-ARC |  | ***Date:*** | 2025-08-15 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | The paper is proposed to resolve security ENs in AIoT procedures.SA3 has made some progress regarding authentication of AIoT Devices and AIoT message protection which are specified in TS 33.369. In procedures of inventory and command, several ENs are removed and some description regarding security is added. |
|  |  |
| ***Summary of change:*** | Clarify the authentication of AIoT Devices and security for the AIoT messages in the inventory and command procedures. |
|  |  |
| ***Consequences if not approved:*** | The authentication of AIoT Devices and security for AIoT messages are not described; and ENs exist. |
|  |  |
| ***Clauses affected:*** | 2, 6.2.2, 6.2.3 |
|  |  |
|  | **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*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.369: “Architecture support for Ambient power-enabled Internet of Things”.

[3] 3GPP TS 38.300: “NR; NR and NG-RAN Overall description; Stage-2”.

[4] 3GPP TS 22.369 “Service requirements for Ambient power-enabled IoT”.

[5] 3GPP TS 33.501 “Security architecture and procedures for 5G System”.

[6] 3GPP TS 38.391: "Ambient IoT Medium Access Control Protocol specification".

[X] 3GPP TS 33.369: "Security aspects of Ambient IoT service".

*NEXT CHANGE*

### 6.2.2 Inventory Procedure

Figure 6.2.2-1 describes the inventory procedure.

The procedure focuses on the messages and parameters used for the communication between AIOTF and NG-RAN regardless of the path to access NG-RAN, see clause 4.2.2.1. The handling of the different communication paths is described in clause 6.2.4.



Figure 6.2.2-1: Inventory Procedure

1. The AF invokes Nnef\_AIoT\_Inventory(AF ID, [External Target Area information], [information about the target AIoT Device(s)], [Approximate number of AIoT Devices], [time interval]) service operation request to the NEF.

 Information about the target AIoT Device(s) may include Filtering Information, as described in clause 5.8, or include complete AIoT Device Identifier(s).

 The approximate number of AIoT Devices, if provided, is used to determine the number of AIoT Devices expected to respond to this inventory service operation, which is sent by AIOTF to the NG-RAN in the assistance information for NG-RAN in step 7 for proper radio resource allocation.

 The time interval, if provided, is described in clause 5.9.

2. The NEF may further authorize the AF request as specified in clause 5.6.

 The NEF determines the Target Area information from the External Target Area information, and selects one or multiple AIOTF(s) to handle the request as specified in clause 5.3.1. The Target Area information is specified in clause 5.3.

3. The NEF invokes the Naiotf\_AIoT\_Inventory(AF ID, [Target Area information], [information about the target AIoT Device(s)], [Approximate number of AIoT Devices], [time interval]) service operation towards to the selected AIOTF(s).

4. The AIOTF receives the AIoT service operation request and checks the parameters included in the request. The AIOTF may perform authorization as specified in clause 5.6. If the AIoT service operation request cannot be processed, the AIOTF rejects the AIoT service operation request with an appropriate cause code, and step 7 onwards are skipped.

 The AIOTF generates a Correlation ID corresponding to this AF service operation request.

 The AIoT Identification Information to be provided to NG-RAN can include Filtering Information, as defined in clause 5.8, or a single AIoT Device Identifier.

 AIOTF performs Reader Selection, see clause 5.3.3.

 The AIOTF may also use the last serving Reader to assist with determining which Readers to use for an AFs request targeting for a specific AIoT Device.

 The AIOTF determines assistance information as described in clause 5.4, taking into account the parameters provided in the service request.

5. AIOTF sends the AIoT Inventory Service Response to the NEF containing the accept or reject result for the AIoT Inventory service operation request based on step 4.

6. NEF sends the AIoT service operation response to the AF, containing the accept or reject result for the AIoT Inventory service operation request as specified in clause 8.3.

NOTE 1: The authentication procedure for the AIoT Devices as specified in clause 5.2 of TS 33.369 [X] is integrated in the following steps.

7. The AIOTF sends the Inventory Request message including the Correlation ID, the AIoT Identification Information to be included in the paging message, and assistance information to the selected NG-RAN as specified in TS 38.413 [10].

8. 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 as specified in TS 38.413 [10].

9. Upon reception of the Inventory Request message from the AIOTF, the RAN Reader(s) will execute the inventory operation as specified in TS 38.300 [5] and TS 38.391 [11]. The RAN Reader(s) broadcast the paging message that includes the AIoT Identification Information.

 The AIoT Device determines whether it matches the AIoT Identification Information, as described in clause 5.8.

 If an AIoT device matches the AIoT Identification Information in the paging message, the AIoT Device responds to the paging message and sends an AIOT NAS message that includes its AIoT identity.

Editor's note: Whether and how the Device ID is concealed or encrypted will be determined and aligned with SA WG3.

10. NG-RAN sends one or more Inventory Report messages to the AIOTF including the Correlation ID, Reader ID and the AIOT NAS message(s) from the AIoT Device(s) as specified in TS 38.413 [10]. The NG-RAN may aggregate multiple Inventory Report messages based on the assistance information before reporting the response to the AIOTF as described in clause 5.9. The AIOTF stores the mapping between the Reader ID and AIoT Device ID(s).

NOTE 2: When to erase the stored mapping between the Reader ID and AIoT device ID(s) is up to implementation and local configuration.

11. The AIOTF validates the results, using local stored device information or device profile data retrieved from the ADM. The AIOTF may aggregate the results.

12. Optionally, if the NG-RAN detects that no more AIoT Devices will respond to the inventory procedure, the NG-RAN informs the AIOTF that the procedure is complete and the last inventory result. After the procedure has completed NG-RAN will not send any further Inventory Reports for this requested Inventory.

Editor's note: The details about completion of the procedure need to be aligned with RAN.

13. The AIOTF reports the progress of the AIoT inventory request to the NEF by sending the Naiotf\_AIoT\_Notify message including a list of AIoT Device Permanent Identifier (s). The AIOTF may send multiple reports. The AIOTF in the final Naiotf\_AIoT\_Notify message indicates it is the last report for this operation. If multiple AIOTFs are involved in the procedure, the NEF may receive the AIoT\_Notify from multiple AIOTFs.

14. When receiving the Naiotf\_AIoT\_Notify message from AIOTF, the NEF informs the AF of the outcome of the AIoT\_Inventory request by sending the Nnef\_AIoT\_Notify message(s) including the AIoT Device Permanent Identifier(s). The NEF in the final Nnef\_AIoT\_Notify message indicates that it is the last report for this operation.

*NEXT CHANGE*

### 6.2.3 Command Procedure

Figure 6.2.3-1 depicts the command procedure.

The procedure focuses on the messages and parameters used for the communication between AIOTF and NG-RAN regardless of the path to access NG-RAN, see clause 4.2.2.1. The handling of the different communication paths is described in clause 6.2.4.



Figure 6.2.3-1: Command Procedure

1. The AF sends the Nnef\_AIoT\_Command (in case of untrusted AF) Request (AF ID, Command Type, information about the target AIoT Device(s), [External Target Area information],  [Approximate number of AIoT Devices], [Approximate D2R message size], [Command type specific parameters]) message to NEF.

 Information about the target AIoT Device(s) may include Filtering Information, as described in clause 5.8, or include complete AIoT Device Identifier(s).

 The External Target Area information is specified in clause 5.3.

 The approximate number of AIoT Devices (see clause 5.4), if provided, is used to indicate the number of AIoT Devices expected to respond to this command service operation, which is sent by AIOTF to the NG-RAN in the assistance information as specified in clause 5.4.

 Command Type provides the operation to be performed and the Command type specific parameters provides the required parameters for the operation. The service operations are described in clause 5.2.2.

2. The NEF selects the AIOTF(s) as described in clause 5.3.1. If no AIOTF can be selected, the NEF rejects the AIoT Command request with an appropriate cause code and step 6 is performed before ending the procedure.

3. The NEF sends Naiotf\_AIoT\_Command Request message (AF ID, Command Type, information about the target AIoT Device(s), [Target area information], [Approximate number of AIoT Devices], [Approximate D2R message size], [Command type specific parameters]) message to the selected AIOTF.

4. The AIOTF receives the AIoT command operation request and checks the parameters included in the request. The AIOTF performs NG- RAN and optionally RAN Reader selection as specified in clause 5.3.3. If no NG-RAN or RAN Reader can be selected, the AIOTF rejects the AIoT Command request with an appropriate cause code.

 The AIOTF generates a Correlation ID corresponding to this AF service operation request, and is used for the AIOTF to correlate the service operation responses to the request.

 The AIOTF determines assistance information as described in clause 5.4.

 The AIOTF performs AF authorization for AIoT command operation as described in clause 5.6.

 The AIOTF performs AMF selection as described in clause 5.3.4.

5. AIOTF sends the Naiotf\_AIoT\_Command Response message (accept or reject, [cause code]) to the NEF.

6. NEF sends the Nnef\_AIoT\_Command Response message (accept or reject, [cause code]) to the AF. If the response was a reject the procedure stops here.

7. Step 7 to step12 of procedure for Inventory specified in clause 6.2.2 are performed with the following clarifications:

- In step 7, the AIOTF also includes follow on command indication in the Inventory Request message to inform the NG-RAN command delivery occurs after the inventory.

- In step 10, the NG-RAN also includes the RAN AIoT Device NGAP ID for each AIoT Device in the Inventory Report as specified in TS 38.413 [10].

- In step 11, the AIOTF validates the results as specified in TS 33.369 [9], and determines whether the command should be sent to an AIoT Device, e.g., by checking the Target AIoT device information. The AIOTF updates the corresponding AIoT device context in the AIOTF to include the RAN AIoT Device NGAP ID.

If none of successful Inventory response is received, Step 8 -11 is not performed and the AIOTF sends a failure report to the NEF in step 12.

8. For each successful Inventory response received, the AIOTF sends Command Request message (Correlation ID, [Reader ID], NAS Command Request, [Approximate D2R message size], RAN AIoT Device NGAP ID for each AIoT Device) to the NG-RAN directly or as a NGAP AIoT information via an AMF as specified in clause 6.2.4. The NAS Command Request message includes the AIoT data. The Correlation ID is as the same as the Correlation ID generated in step 4. The RAN AIoT Device NGAP ID for each AIoT Device is used by the NG-RAN to determine the AIoT device context in NG-RAN as specified in TS 38.413 [10].

 The AIOTF uses the Command Type and Command type specific parameters received in Step 3 to determine the NAS Command Request to send to the AIoT Device, as described in clause 5.2.2.

 The protection of the NAS Command Request message is specified in clause 5.3 of TS 33.369 [X].

NOTE: Command Request(s) can be sent to NG-RAN when inventory procedure is ongoing.

9. The NG-RAN sends the AS R2D message (NAS Command Request) to the AIoT Device as defined in TS 38.391 [11].

10. The AIoT Device sends the AS D2R message (NAS Command Response) to the NG-RAN as defined in TS 38.391 [11]. The NAS Command Response message may include the AIoT data.

 The protection of the NAS Command Response message is specified in clause 5.3 of TS 33.369 [X].

11. The NG-RAN responds with a Command Response message (Correlation ID, Reader ID, NAS Command Response, RAN AIoT Device NGAP ID) to the AIOTF directly or as a NGAP AIoT information via an AMF as specified in clause 6.2.4. The AIOTF determines the AIoT device context by the RAN AIoT Device NGAP ID received.

12. The AIOTF reports the result of the AIoT Command request to the NEF by sending the Naiotf\_AIoT\_Command Notify message (a list of AIoT Device(s) response information (AIoT Device ID(s), AIoT data), AF ID, [Last Report Indication]).

13. The NEF informs the AF of the result of the AIoT\_Command request by sending the Nnef\_AIoT\_Command Notify message (a list of AIoT Device(s) response information (AIoT Device ID(s), AIoT data), AF ID, [Last Report Indication]).

*END OF CHANGES*