ETSI TS 123 369 V19.4.0 (2026-07)

TECHNICAL SPECIFICATION

5G;
Architecture support
for Ambient power-enabled Internet of Things;
Stage 2
(3GPP TS 23.369 version 19.4.0 Release 19)

Reference
RTS/TSGS-0223369vj40

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies architectural enhancements to the 5G system to support Ambient power-enabled Internet of Things, complying to the requirements in TS 22.369 [2] applicable to the AIoT Device types, traffic types, use cases and connectivity topologies defined in TS 38.300 [5].

In this Release, the AIoT system is defined as an isolated private network, such as SNPN, that does not interact with a public network.

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 22.369: "Service requirements for Ambient power-enabled IoT".

[3] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TS 38.300: "NR; Overall description; Stage-2".

[6] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[7] GS1 TDS Release 2.1: "EPC Tag Data Standard".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] 3GPP TS 33.369: "Security aspects of Ambient Internet of Things (AIoT) services for isolated private networks".

[10] 3GPP TS 38.413: "NG Application Protocol (NGAP)".

[11] 3GPP TS 38.391: "Ambient IoT Medium Access Control Protocol specification".

[12] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[13] 3GPP TS 24.369: "Ambient IoT Non-Access-Stratum (AIoT NAS) protocol for 5G System (5GS); Stage 3".

3 Definitions of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

AIoT Area: An area in which NG-RAN can perform Ambient IoT operations, see TS 38.300 [5], represented by an AIoT Area identifier. There can be multiple NG-RAN nodes and multiple RAN Readers in a single AIoT Area. NG-RAN nodes and RAN Readers can be part of multiple AIoT Areas.

AIoT Device: An Ambient IoT device is an IoT device powered by energy harvesting, with limited energy storage capability.

External Area Identifier: An identifier for an AIoT service area used by the AF when requesting AIoT Service Operations.

External Target Area: An area used between the NEF and AF in AIoT service operations, identified by a pre-configured External Area Identifier or geographic location (e.g. a civic address or GAD shapes, see TS 23.032 [12]).

Target Area: An area in which a service operation request towards an AIOTF is intended to operate, identified by a list of AIoT Areas.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ADM	AIoT Data Management
AIoT	Ambient IoT
AIOTF	Ambient IoT Function
EPC	Electronic Product Code

4 Architecture model and concepts

4.1 General concept

AIoT is a service that can be provided by the 5GS system to support Ambient power-enabled IoT devices that are powered by energy harvesting, being either battery-less or with limited energy storage capability (e.g. using a capacitor) and the energy is provided through the harvesting of radio waves, light, motion, heat, or any other suitable power source.

The 5GS System architecture for AIoT include the following functions and procedures for:

- AIoT Device identification;
- AIoT Device inventory;
- Providing to, and obtaining from, an AIoT Device application data.
- Disabling AIoT Devices.

4.2 Architecture

4.2.1 General

The 5GS System architecture for AIoT includes core network functions, different AIoT Reader architectures and AIoT Devices. The different AIoT Reader architectures allow for different deployment options. The following AIoT Reader architectures are defined:

- NG-RAN (which supports AIoT Reader), which includes either a direct connectivity between NG-RAN and the AIOTF or an indirect connectivity between NG-RAN and the AIOTF via an AMF.

The NG-RAN in this specification refers to the gNB which supports AIoT related functionalities, as specified in TS 38.300 [5]. The gNB may only support communication with AIoT Devices.

The architecture for Network Exposure Function, using reference point representation, defined in clause 4.2.3 of TS 23.501 [3] is applicable for AIoT, with a southbound interface from the NEF to AIOTF.

4.2.2 Architecture for NG-RAN connectivity

4.2.2.1 General

5GS system architecture for AIoT supports the following connectivity to access an NG-RAN:

- Direct Connectivity: AIOTF communicates with NG-RAN directly.
- Indirect Connectivity via AMF: NG-RAN and the AIOTF communicate indirectly via an AMF.

Figure 4.2.2.1-1 depicts the complete non-roaming architecture showing the overall 5GS architecture for support of AIoT, including both the Indirect Connectivity and Direct Connectivity.

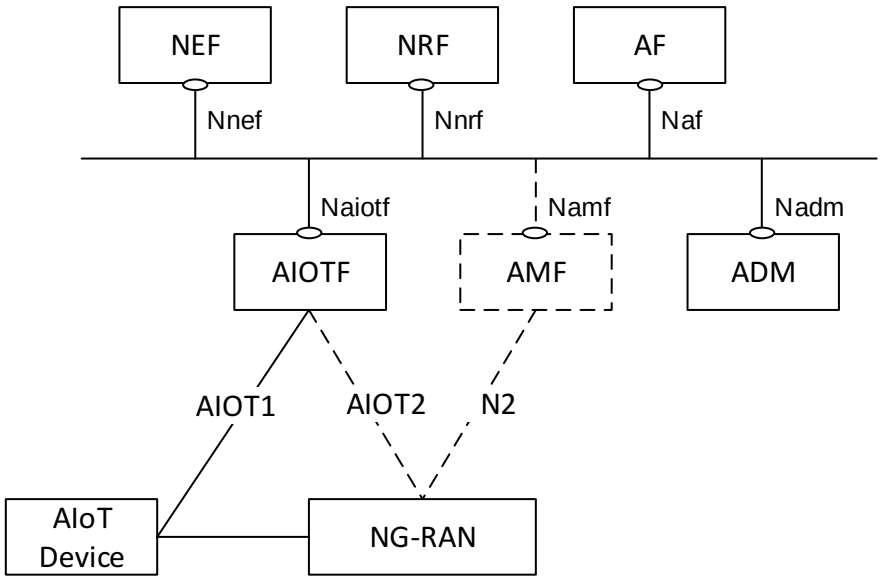


Figure 4.2.2.1-1: Non-roaming AIoT System Architecture

NOTE 1: For the sake of clarity and to depict the complete reference point architecture, the AMF, AIOT2 and N2 as depicted using dashed lines, as all deployments might not use them.

Figure 4.2.2.1-2 depicts the complete non-roaming AIoT system architecture, using the reference point representation.

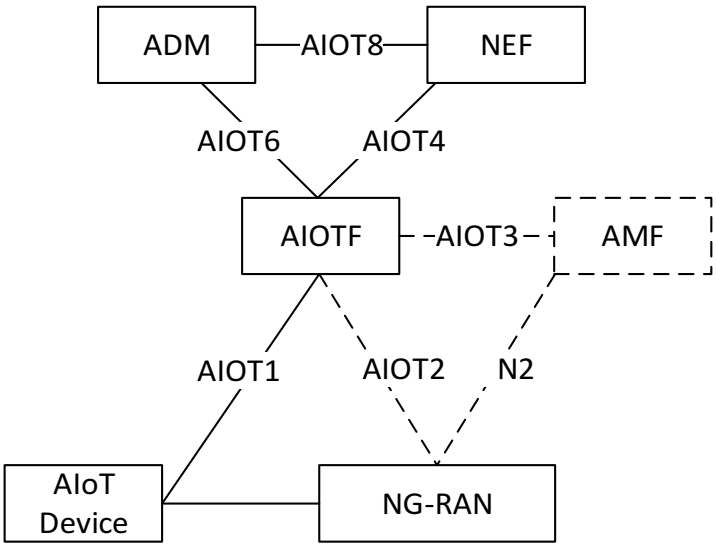


Figure 4.2.2.1-2: Non-roaming AIoT System Architecture (RAN Readers) in reference point representation

NOTE 2: For the sake of clarity of the point-to-point diagrams, the AF and NRF have not been depicted. However, all depicted Network Functions can interact with the NRF as necessary.

NOTE 3: For clarity, the UDR and its connections with ADM, are not depicted in the point-to-point and service-based architecture diagrams. For more information on the ADM data storage architectures refer to clause 4.5.8.

NOTE 4: For the sake of clarity and to depict the complete reference point architecture, the AMF, AIOT3, N2 and AIOT2 as depicted using dashed lines, as all deployments might not use them.

The architectures in the following clauses showing parts of the overall AIoT architecture specific to each connectivity option:

- Direct Connectivity: the AIOTF uses AIOT2 to access NG-RAN, and is described in clause 4.2.2.2.
- Indirect Connectivity via AMF: the AIOTF uses an AMF which uses N2 to access NG-RAN, and is described in clause 4.2.2.3.

NOTE 5: A deployment that only uses, e.g. the Direct Connectivity only does not need to deploy the NFs, reference points and service-based interfaces associated with the Indirect Connectivity, and vice-versa.

4.2.2.2 Direct Connectivity between AIOTF and NG-RAN

In the Direct Connectivity architecture, the AIOTF uses AIOT2 to communicate directly with NG-RAN.

Figure 4.2.2.2-1 depicts the AIoT architecture, using the service-based interfaces, showing only the parts of the AIoT architecture for an AIOTF connecting to NG-RAN directly. The remaining parts of the AIoT architecture shown in Figure 4.2.2.1-1 remain unchanged.

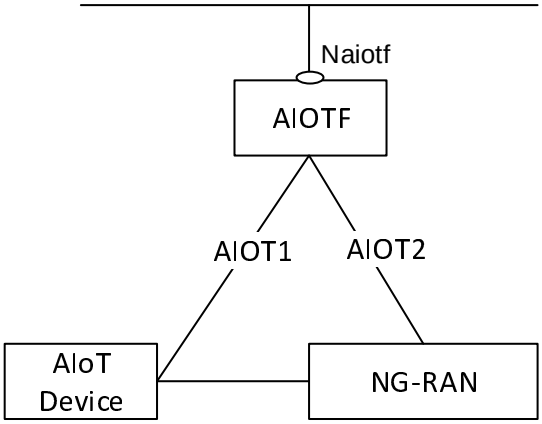


Figure 4.2.2.2-1: NG-RAN - AIOTF Direct Connectivity Architecture

Figure 4.2.2.2-2 depicts the AIoT architecture, using the reference point representation, showing only the parts of the AIoT architecture for an AIOTF access NG-RAN. The remaining parts of the AIoT architecture shown in Figure 4.2.2.1-2 remain unchanged.

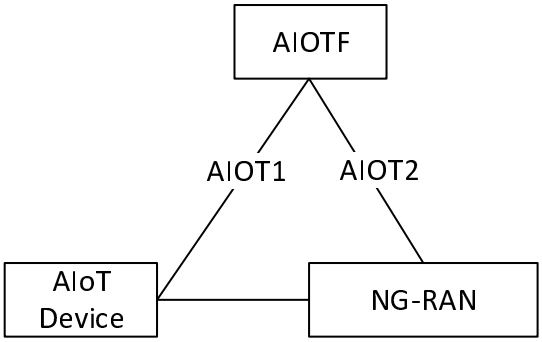


Figure 4.2.2.2-2: NG-RAN - AIOTF Direct Connectivity Architecture in reference point representation

4.2.2.3 Indirect Connectivity between AIOTF and NG-RAN via an AMF

Figure 4.2.2.3-1 depicts the AIoT architecture, using the service-based interfaces showing only the parts of the AIoT architecture for an AIOTF connects indirectly to NG-RAN via an AMF. The remaining parts of the AIoT Architecture shown in Figure 4.2.2.1-1 remain unchanged.

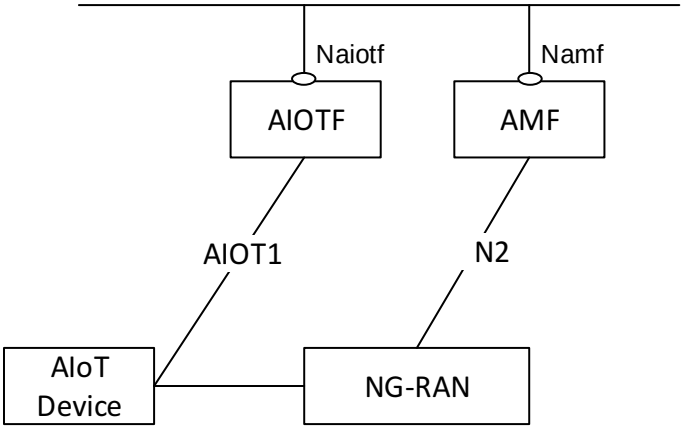


Figure 4.2.2.3-1: NG-RAN - AIOTF Indirect Connectivity Architecture

Figure 4.2.2.3-2 depicts the AIoT architecture, using the reference point representation showing only the parts of the AIoT architecture for an AIOTF connects to NG-RAN via an AMF. The remaining parts of the AIoT architecture shown in Figure 4.2.2.1-2 remain unchanged.

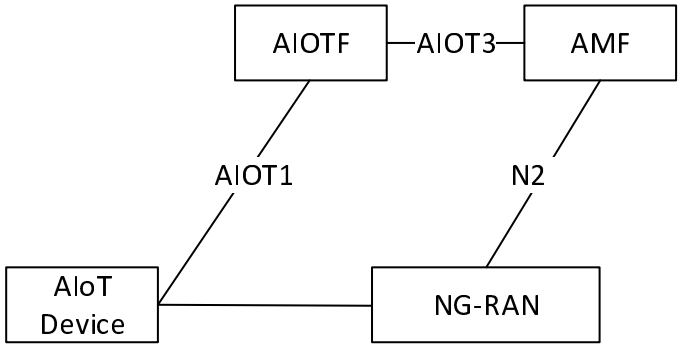


Figure 4.2.2.3-2: NG-RAN - AIOTF Indirect Connectivity Architecture in reference point representation

4.3 Reference points

The AIoT Architecture contains the following reference points:

AIOT1: Reference point between the AIoT Device and the AIOTF.

AIOT2: Reference point between the NG-RAN and the AIOTF.

The following reference points show the interactions that exist between the NF services in the NFs. These reference points are realized by corresponding NF service-based interfaces and by specifying the identified consumer and producer NF service as well as their interaction in order to realize a particular system procedure.

AIOT3: Reference point between the AIOTF and the AMF.

AIOT4: Reference point between the AIOTF and the NEF.

AIOT5: Reference point between the AIOTF and the NRF.

AIOT6: Reference point between the AIOTF and the ADM.

AIOT7: Reference point between the ADM and the UDR.

AIOT8: Reference point between the ADM and the NEF.

In addition to the relevant reference points defined in TS 23.501 [3], in the case of AIoT, these reference points are as follows:

N2: Reference point between the NG-RAN and the AMF.

N33: Reference point between NEF and AF.

4.4 Service-based interfaces

Naiotf: Service-based interface exhibited by the AIOTF.

Nadm: Service-based interface exhibited by the ADM.

In addition to the relevant services defined in TS 23.501 [3] the following service-based interfaces are enhanced for AIoT in this specification:

Namf: Service-based interface exhibited by AMF.

Nnef: Service-based interface exhibited by NEF.

Naf: Service-based interface exhibited by AF.

Nnrf: Service-based interface exhibited by NRF.

4.5 Functional Entities

4.5.1 AIoT Device

The AIoT Device supports the following functionality:

- Support of AIoT NAS protocol with the AIOTF.
- Support of AIoT radio interface towards AIoT reader, as defined in TS 38.300 [5].

4.5.2 NG-RAN

The NG-RAN in this specification refers to the gNB which supports AIoT related functionalities as specified in clause 4.2.1.

The NG-RAN supports the following functions:

- The NG-RAN communicates with the AIOTF either via direct connectivity or indirect connectivity.
- The NG-RAN serves one or more AIoT readers.
- The NG-RAN supports the inventory and command procedures.
- The NG-RAN supports the functionalities defined in TS 38.300 [5].
- The NG-RAN and AIoT readers may aggregate data collected from multiple AIoT Devices in accordance with the assistance information as specified in clause 5.9.

4.5.3 AIOTF

The AIOTF supports the following functions:

- Termination of AIoT NAS protocol with AIoT Device.
- Connectivity with an NG-RAN via a direct interface reference point or via an AMF.
- Support of AIoT service operations towards the AIoT Devices(s):
  - Providing an interface to the AF (or via NEF) for AIoT services and authorizing the trusted AF's AIoT service operation requests.
  - Triggering the NG-RAN to perform AIoT service operations towards the AIoT Device(s), and optionally determining and providing assistance information to the NG-RAN.
  - Report the service operation results based on the local configuration or the request.
  - NG-RAN selection and optionally a list of RAN Reader selection for AIoT service operations.
  - AMF selection based on target area information when AIOTF connects to NG-RAN indirectly via an AMF.
  - Correlation ID allocation corresponding to the AF service operation request.
- Retrieving AIoT Device Profile Data from ADM.
- Retrieving AF subscription data from ADM.
- Optionally AIoT Device context management.
- Perform aggregation of the AIoT service responses, determine and provide assistant for the AIoT aggregation in NG-RAN.

NOTE: Authentication of AIoT Devices related to AIOTF is defined in TS 33.369 [9].

4.5.4 NEF

In addition to the functions defined in TS 23.501 [3], the NEF performs the following functions:

- Providing a service exposure API to AFs of 3rd party for AIoT services.
- Interacting with AF of 3rd party and AIOTF.
- Selection of AIOTF for AIoT services.
- Authorization of the untrusted AF's AIoT service operation requests.

4.5.5 AF

The AF performs the following functions to support AIoT services:

- Interacting with NEF for AIoT related service exposure for 3rd party .
- Interacting with AIOTF for AIoT related service exposure for trusted AF.

4.5.6 NRF

In addition to the functions defined in TS 23.501 [3], the NRF performs the following functions:

- Support of the AIOTF NF type and its corresponding NF profile. The NF profile includes the AIOTF ID, FQDN or IP address, NF type and the serving area information of the AIOTF.

NOTE: The serving area information of the AIOTF is constructed by the sum of the supported AIoT serving area of the NG-RAN nodes that are directly or indirectly connected to the AIOTF.

- Support of AIOTF discovery based on Target Area information.
- Support of the ADM NF type and its corresponding NF profile. The NF profile includes the ADM ID, FQDN or IP address, NF type, the supported Domain Information of AIoT Device Permanent Identifiers, the supported AIoT Device Permanent Identifier ranges, and optionally the supported AF IDs.
- Support of ADM discovery based on parameters as specified in clause 5.3.2.

The AIOTF(s) and the ADM register or update its NF profile in the NRF by means of the method as defined in clause 4.17.2 of TS 23.502 [4].

4.5.7 AMF

The AMF performs the following functions when the NG-RAN and the AIOTF communicate indirectly via an AMF:

- Relaying signalling for AIoT service (including e.g., inventory/command messages) between NG-RAN and AIOTF transparently.
- Providing transparent transport for AIoT NAS messages between AIoT Device and AIOTF.

4.5.8 UDR

In addition to the functions defined in TS 23.501 [3], the UDR may support the following functions:

- Storage of Ambient IoT data, including:
  - AIoT Device Profile Data.
  - AF authorization data.

4.5.9 ADM

The ADM supports the following functions:

- Management of AIoT Device Profile Data.
- Management of AIoT Device security data including device credentials as defined in clause 4.2.3 of TS 33.369 [9].
- Management of AF authorization data.

The AIoT Device Profile Data and AF authorization data used by the ADM may be stored in the UDR.

4.6 Protocol Stacks

4.6.1 General

This clause specifies the protocol stacks among entities used for AIoT. The protocol stacks include the following:

- Protocol stacks between AIoT Device and AFs, including the protocol stacks among AIoT Device, NG-RAN, AMF, AIOTF, NEF and AFs.

4.6.2 Protocol Stack between AIoT Device and AF

4.6.2.1 General

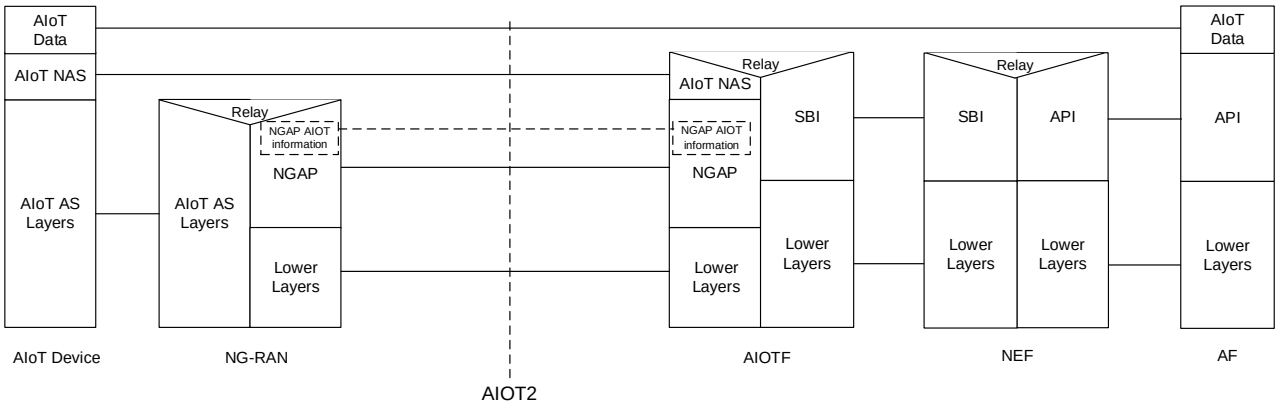
The NG-RAN communicates with AIOTF via one of the two connectivity options as following:

- Direct Connectivity: When the NG-RAN communicates with AIOTF directly, the protocol stack is specified in clause 4.6.2.2.
- Indirect Connectivity: When the NG-RAN communicates with AIOTF indirectly via an AMF, the protocol stack is specified in clause 4.6.2.3.

For both connectivity options, NG-RAN communicates with AIOTF or AMF via NGAP as specified in TS 38.413 [10].

The AIoT NAS protocol supports the Inventory and Command related procedures as defined in clause 6.

4.6.2.2 Protocol Stack between AF and AIoT Device for NG-RAN Direct Connectivity



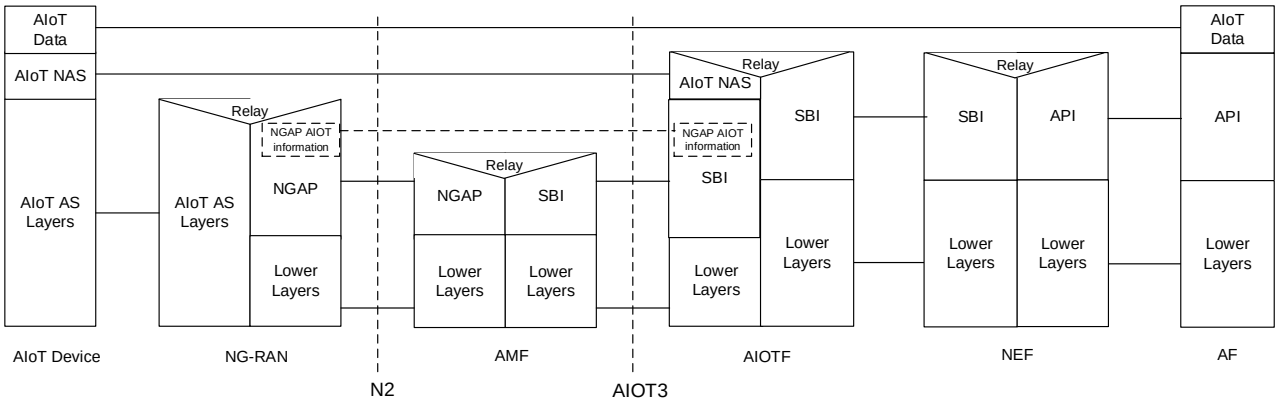
Legend:

- **AIoT Data:** It is the application data exchanged between the AIoT Device and the AF.
- **AIoT NAS:** The NAS protocol between AIoT Device and the AIOTF.
- **AIoT AS:** It is between the AIoT Device and the NG-RAN as specified in TS 38.300 [5].
- **NGAP:** Application Layer Protocol between the AIOTF and the NG-RAN as defined in TS 38.413 [10].
- **NGAP AIoT Information:** It is the subset of NGAP information and is included in the NGAP messages over AIOT2 reference point.

Figure 4.6.2.2-1: Protocol Stack between AF and AIoT Device for Direct Connectivity option

The AIoT NAS messages between the AIoT Device and the AIOTF are transferred via the NG-RAN transparently.

4.6.2.3 Protocol Stack between AF and AIoT Device for NG-RAN Indirect Connectivity



Legend:

- **AIoT Data:** It is the application data exchanged between the AIoT Device and the AF.
- **AIoT NAS:** The NAS protocol between AIoT Device and the AIOTF.
- **AIoT AS:** It is between the AIoT Device and the NG-RAN as specified in TS 38.300 [5].
- **NGAP:** Application Layer Protocol between the AMF and the NG-RAN as defined in TS 38.413 [10].
- **NGAP AIoT Information:** It is the subset of NGAP information that the AMF transparently relays between the NG-RAN and the AIOTF, and is included in the NGAP messages and the AIOT3 messages.

Figure 4.6.2.3-1: Protocol Stack between AF and AIoT Device for Indirect Connectivity via AMF option

NOTE: From the NG-RAN perspective, there is a single termination of N2 i.e. the AMF.

In the Indirect Connectivity option, the AMF is involved and its functionality is as defined in clause 4.5.7. The AIoT NAS messages between the AIoT Device and the AIOTF are transferred via the NG-RAN and AMF transparently.

5 High level functionality and features

5.1 General

Clause 5 specifies the high-level functionality and features to support Ambient IoT in the 5G system.

5.2 AIoT Services

5.2.0 General

The following AIoT Services are supported:

- Inventory service;
- Command service.

5.2.1 AIoT Inventory service

AIoT Inventory service is used to discover the AIoT Devices.

5.2.2 AIoT Command service

5.2.2.1 Overview

Three types of Command service operations are supported: Read, Write and Disable.

An AF uses the Command service Read operation to retrieve information from AIoT Device(s), and the AIOTF uses the commands described in clause 5.2.2.2 towards the AIoT Device for the operation.

An AF uses the Command service Write operation to write information to AIoT Device(s), and the AIOTF uses the AIoT NAS Commands described in clause 5.2.2.2 towards the AIoT Device for the operation.

An AF uses the Command service Disable operation to permanently disable the capability of AIoT Device(s) to transmit RF signals, and the AIOTF uses the AIoT NAS Commands described in clause 5.2.2.3 towards the AIoT Device for the operation.

If the AIoT Device receives a NAS Command Request that the AIoT Device does not support or has not implemented, the AIoT Device shall return an AIOT STATUS message with an appropriate cause code as defined in TS 24.369 [13]. Otherwise, the AIoT Device performs the Command service operation according to the received NAS Command Request.

5.2.2.2 Read and Write Commands

It is optional for an AIoT Device to support of Read and Write Commands. If supported, an AIoT Device contains User Memory that can be used to store application specific data and is accessed using AIoT NAS Commands from an AIOTF. An AIoT Device implementation may have other storage outside of the User Memory that is used to store e.g. AIoT Device Permanent Identifier, etc.

The User Memory is accessed by the following AIoT NAS Commands and responses between the AIOTF and AIoT Device:

- Read Request: used to read application data from User Memory.
- Read Response: Response from the AIoT Device to Read Request, providing a status and the application data read from the User Memory.
- Write Request: used to write application data to User Memory.
- Write Response: Response from the AIoT Device to Write Request, providing a status for the Write Request.

The Read Request and Response, and Write Request and Response AIoT NAS Commands are used to access the User Memory when an authorized AF uses the Read or Write command service operations, as described in clause 5.2.2.1. The Read or Write Request is sent in the Command Request step and the Read or Write Response is sent in the Command Response step of the Command procedure described in clause 6.2.3.

The physical memory map of an AIoT Device and where the User Memory is within it is implementation specific.

The AIoT NAS Commands to access the User Memory include an offset from the start of the User Memory to indicate where to read application data from and where to write application data to. The offset and the application data transferred in the Read Request, Write Request, and Read Response has no special meaning to the network, and the AIOTF or other NFs do not attempt to interpret them.

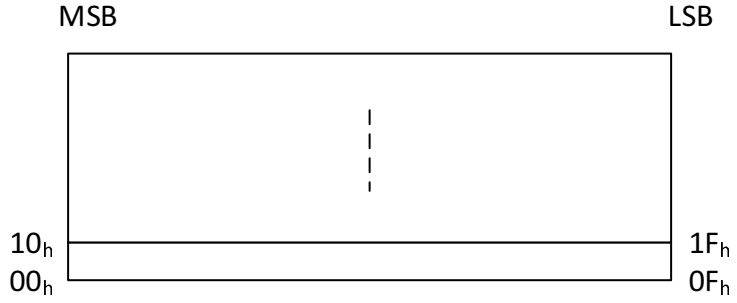


Figure 5.2.2.2-1: Logical AIoT Device User Memory

The Write Request command is used to write application data into the User Memory and includes:

- the application data to write and its length; and

- the offset where to write the application data.

The AIoT Device responds with a Write Response indicating whether the Write Request was successful.

The Read command is used to read from the User Memory and includes:

- the offset to read application data from; and
- the length of the application data to read.

The application data is from the User Memory in the place indicated by the offset and the length.

The AIoT Device responds with a Read Response including whether the read was successful and the application data read from the User Memory.

If an AIoT Device does not support Read Request or Write Request commands, or the parameters in the commands are invalid the AIoT Device shall reject the command.

5.2.2.3 Permanent Disable Command

An AIoT Device may be permanently disabled. A permanently disabled AIoT Device does not respond to the inventory procedure, as described in clause 6.2.2.

An AIoT Device is permanently disabled by the Permanent Disable AIoT NAS Command sent by an AIOTF to the AIoT Device.

The Permanent Disable AIoT NAS Command is sent to an AIoT Device when an authorized AF uses the Permanent Disable command service operations as described in clause 5.2.2.1, or if the network determines to disable the AIoT Device. The Permanent Disable AIoT NAS Command is sent in the Command Request step and a response is sent in the Command Response step of the Command procedure described in clause 6.2.3. The AIoT Device responds indicating whether the Permanent Disable command was successful.

NOTE: The trigger conditions when a network determines to disable the AIoT Device depends on operator and implementation policy.

When the AIoT Device has received and verified a Permanent Disable AIoT NAS Command, it shall no longer respond to the inventory procedure.

5.3 Discovery and Selection of AIoT node(s)

5.3.1 AIOTF Discovery and Selection

The AIOTF discovery and selection functionality is used to determine AIOTF instances(s) to handle an AIoT service operation request.

The NEF determines AIOTF instances(s) by providing the NRF with Target Area information and the NRF returning AIOTF instance(s) that match the provided Target Area information, or by using local configuration.

A service operation request received by the NEF from an AF may include External Target Area information and the NEF uses it to determine the Target Area information that is provided to the AIOTF and NRF, if used. The External Target Area information is a pre-configured External Area Identifier or geographic area (e.g., a civic address or GAD shapes). The Target Area information is a list of AIoT Areas.

NOTE: The mapping between AIoT Areas and External Area Identifiers information provided by an AF is configured in the NEF.

When an AIoT service operation request indicates individual AIoT Device(s), the AIOTF instance(s) may be selected by taking into account the last known AIOTF instance(s) (e.g. AIOTF ID/address) for those AIoT Device(s) obtained from the ADM.

5.3.2 ADM Discovery and Selection

The ADM discovery and selection function is supported by the AIOTF to select an ADM instance to retrieve the AIoT Device Profile Data or update the last known AIOTF for the AIoT Device. The AIOTF may also discover and select an ADM to retrieve AF authorization data. Similarly, the NEF uses the ADM discovery and selection function to select an ADM to obtain the last known AIOTF for the AIoT Device.

When the ADM discovery is performed, the AIOTF or the NEF utilizes the NRF to discover the ADM instance(s) unless the ADM information is available by other means, e.g., locally configured. The AIOTF or the NEF selects an ADM instance based on the available ADM instances (obtained from the NRF or locally configured).

The following factors may be considered for the ADM discovery and selection for AIoT Device Profile Data retrieval or update:

- The Domain Information or the AIoT Device Permanent Identifier.

NOTE 1: Based on local configuration, the AIOTF or the NEF can determine whether to use the Domain Information or the AIoT Device Permanent Identifier.

NOTE 2: In case the Domain Information is empty, the AIOTF or the NEF uses AIoT Device Permanent Identifier for ADM discovery and selection.

The following factors may be considered for the ADM discovery and selection for AF authorization data retrieval:

- The AF ID.

5.3.3 NG-RAN Node and RAN Reader Selection

The AIOTF selects NG-RAN node(s) and optionally RAN Readers based on the configured NG-RAN configuration information and the received AIoT service operation request. The AIOTF may also select a RAN Reader based on the stored last known RAN Reader information.

The AIOTF obtains the NG-RAN configuration information that can be used for selection. For each NG-RAN node, the following is provided:

- Served AIoT Area ID List of the NG-RAN node: The AIoT Areas that are not configured in the RAN Reader List, e.g. when RAN Reader List is not configured.

- RAN Reader List: For each RAN Reader, the following information is provided:

- Served AIoT Area ID List of the RAN Reader.

- Optionally, location information.

For each NG-RAN node, the AIOTF obtains a served AIoT Area ID List of the NG-RAN node, a RAN Reader List, or both. The provisioning of the NG-RAN configuration information can be performed via OAM or local configuration.

When the AIOTF receives an AIoT service operation request, based on the received Target Area information in the AIoT service operation request and the NG-RAN configuration information, the AIOTF selects the NG-RAN node(s) and optionally RAN Reader(s) to handle the request and the AIOTF determines a Requested Service Area Information for each selected NG-RAN node. The Requested Service Area Information provided by the AIOTF to each selected NG-RAN node can be empty, or includes a list of AIoT Area IDs, a list of RAN Reader IDs, or both a list of AIoT Area IDs and a list of RAN Reader IDs. How the NG-RAN node determines RAN Readers based on the Requested Service Area Information is specified in TS 38.300 [5].

NOTE 1: The Target Area information in a received AIoT service operation request can span multiple NG-RAN node(s) or can be a subset of the supported AIoT areas of a single NG-RAN node.

The AIOTF sends the AIoT service operation request to each selected NG-RAN node, either directly or through the selected AMF, including the Requested Service Area Information for the NG-RAN node.

If an AIoT service operation request received by the AIOTF includes individual target AIoT Device Permanent ID(s), the AIOTF may consider the last known serving RAN Reader, if available from the AIoT Device context to determine the NG-RAN node and RAN Reader(s) for the request. In this case the last known serving RAN Reader ID is sent as the Requested Service Area to the selected NG-RAN node.

NOTE 2: The RAN Reader ID is not exposed to the AF.

NOTE 3: An AIOTF receives the Inventory Report from an NG-RAN node includes a RAN Reader ID that represents the AIoT Device's location at Reader granularity.

NOTE 4: The AIOTF uses the RAN Reader ID and the NG-RAN node to update the last known serving RAN Reader information in the local AIoT Device context.

5.3.4 AMF Discovery and Selection

For Indirect Connectivity via AMF (see clause 4.2), AMF discovery and selection functionality is implemented in AIOTF.

In this case, the AIOTF is locally configured with the information of the AMF corresponding NG-RAN node(s).

The AIOTF selects the AMF that is corresponding to the selected NG-RAN nodes based on the local configuration in order to forward the AIoT service operation messages towards the selected NG-RAN node(s) (see NG-RAN Node and RAN Reader Selection in clause 5.3.3) via the selected AMF.

NOTE: It is left to stage3 to handle the case that the AMF fails to forward the inventory or command request to the selected NG-RAN. It is up to the operator to ensure local configured AMF corresponding to the NG-RAN do have the NG connection with the AMF during the deployment phase.

5.4 Assistance information provided to NG-RAN node

The AIOTF provides the following assistance information to the NG-RAN together with the service operation requests.

For Inventory or Command service operation, following Inventory Assistance Information is included in the Inventory Request from AIOTF to NG-RAN:

a) Optionally, approximate number of AIoT Devices based on AF request.

b) Size of the AIoT NAS Inventory Report message from the AIoT Device.

c) Optionally, time interval for AIoT Device response aggregation used by the NG-RAN as specified in clause 5.9.

For Command service operation, following Command Assistance Information is included in the Command Request from AIOTF to NG-RAN:

d) Size of the Command Response message from the AIoT Device.

Bullet b) is determined by AIOTF based on the length of device specific authentication information as specified in TS 33.369 [9] and if AIoT Device ID Permanent ID is included, its length is considered.

If not provided by the AF, bullet c) in the above assistance information provided by the AIOTF may be based on local configuration based on SLA between the AIoT service provider represented by an AF and the operator.

The assistance information is used by the NG-RAN for performing service operations, e.g. radio resource allocation by using bullets a), b) and d), AIoT Device responses aggregation by using bullet c).

5.5 AIoT Device Profile Management

The ADM may hold AIoT Device Profile Data for the AIoT Device used in the network. If the AIoT Device is managed by the network, then the profile data for an AIoT Device is managed in the ADM, otherwise the corresponding profile data is stored external to the network.

The AIoT Device Permanent Identifier is used by the AIOTF together with local configuration, 3rd party related context to locate the entity which stores the profile data of an AIoT Device.

In case the AIoT Device is managed by the network, the AIOTF checks whether the AIoT Device Permanent Identifier from AIoT Device has the profile data in the network and retrieves the AIoT Device Profile Data. The AIoT Device Profile Data for AIoT Devices is different from the UE subscription data as defined in clause 5.2.3 of TS 23.502 [4], it

is stored in the ADM network entity that exclusively supports management of AIoT Device Profile Data. The AIoT Device Permanent Identifier is the primary key for AIoT Device Profile Data in the ADM.

Optionally, the ADM stores AIoT Device Temporary Identifier(s) as described in TS 33.369 [9].

The table 5.5-1 below describes information storage structures for AIoT Device Profile Data.

Table 5.5-1: AIoT Device Profile Data

Field	Description
AIoT Device Permanent Identifier	Uniquely identifies the AIoT Device.
Last known AIOTF information	Indicate the last known AIOTF that served the AIoT Device, or unknown
AIoT Device Temporary Identifier(s)	Temporary Identifier(s) may be stored as described in TS 33.369 [9].

NOTE: In addition to the AIoT Device Profile Data, the ADM also manages AIoT Device security data including device credentials as specified in TS 33.369 [9].

5.6 AF authorization for AIoT Services

The information needed to support the authorization of the AF for AIoT services is stored as the authorization data for 3rd party AF in the ADM, or locally configured in the AIOTF.

Table 5.6-1 below describes items stored as AF authorization data for the AIoT.

Table 5.6-1: AF Authorization Data for AIoT

AF Authorization Data	Description
AF ID	Identifier used to identify the AF.
Allowed area	Indicate the allowed area for the indicated AF to request the AIoT services.
Allowed service operations	Indicate the allowed service operation(s) for the indicated AF, e.g. inventory, read, write, permanent disable.
Allowed target AIoT Devices	Indicate the allowed AIoT Device(s) for the indicated AF. The information indicating the allowed target AIoT Devices is a list of the permanent AIoT Device ID (see clause 5.7) or the filtering information (see clause 5.8).

The authorization of the AF for AIoT services includes two parts:

- NEF performs AIoT AF request authorization based on the service level agreement (SLA) between the 3rd party AF and the 5GS of the mobile network operator, the operator policy and local configuration as in TS 33.501 [8].
- AIOTF may perform authorization of AIoT service requested by the AF, using the AF authorization data retrieved from the ADM or configured locally as described in above Table 5.6-1. When an ADM is used, the AIOTF also subscribes to changes of AF authorization data in the ADM for synchronization.

5.7 Identifiers

5.7.1 General

The following clauses define the identifiers used within the AIoT system to support identification of AIoT Devices and AIoT Sessions.

5.7.2 AIoT Device Permanent Identifier

In order to support the AIoT feature in 5G System, a globally unique AIoT Device Permanent Identifier shall be allocated to each AIoT Device. An AIoT Device Permanent Identifier is assigned either by an operator or by a third party. The AIoT Device Permanent Identifier is used to identify an AIoT Device and locate the entity where the AIoT Device related information is stored.

NOTE 1: How to configure an AIoT Device with the AIoT Device Permanent Identifier is out of scope of this specification.

The AIoT Device Permanent Identifier includes the following components:

- The ID Type, including:
  - Information indicating whether a PLMN ID is included.
  - Information indicating whether a NID is included.
  - Information indicating whether a Third Party Identifier is included.
  - Identification Information Type, indicating whether the Identification Information contains an EPC or unstructured information.
  - Information indicating the length of Identification Information.
- The Domain Information includes none, one or more of the following:
  - A PLMN Identifier (i.e., MCC and MNC) as specified in TS 23.003 [6] when the information in the ID type indicates it is included
  - A Network Identifier (NID) as specified in TS 23.003 [6] when the information in the ID Type indicates it is included.
  - A Third Party Identifier used to identify a third party when the information in the ID Type indicates it is included.
- The Identification Information is used to distinguish different AIoT Devices within the scope identified by Domain Information (if available) and can contain either:
  - An EPC, as defined in clause 14 of GS1 TDS Release 2.1 [7].
  - Unstructured information, where the contents are defined by the allocator.

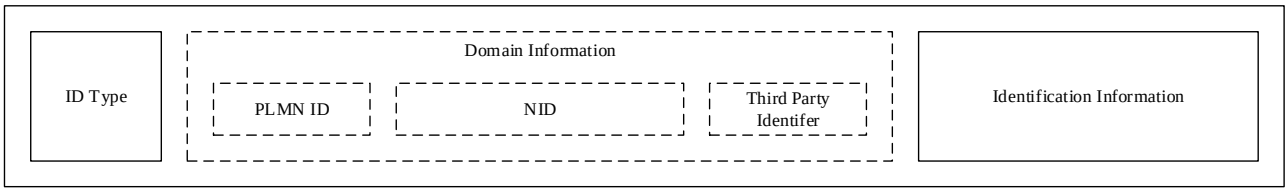


Figure 5.7.2-1: AIoT Device Permanent Identifier Structure

An operator allocated AIoT Device Permanent Identifier should include the identifier of the network for the operator. The identifier of the network is present as either a PLMN Identifier, NID or both in the AIoT Device Permanent Identifier.

A third party allocated AIoT Device Permanent Identifier may include none or any combination of at least one of the following: a PLMN Identifier, NID or Third Party Identifier.

NOTE 3: The length of ID Type, PLMN Identifier (if present), NID (if present) and the Third Party Identifier (if present) components are fixed. The length of the Identification Information is variable. The details are specified in TS 23.003 [6].

NOTE 4: When the Domain Information is empty, the AIOTF uses, e.g., Identification Information (i.e. EPC) to discover and select the ADM instance or the external server for the AIoT Device Profile Data.

The following lengths are supported for the Identification Information in an AIoT Device Permanent Identifier: 32 bits, 64 bits, 96 bits, 128 bits, 256 bits and 496 bits.

NOTE 5: The encoding for the length of the Identification Information enables additional shorter or longer fixed lengths to be supported in the future.

5.7.3 Correlation ID

Correlation ID is generated by AIOTF corresponding to an AF service operation request. It is used together with AIOTF ID to uniquely identify an AIoT Session between the NG-RAN and AIOTF which is corresponding to an AF service operation request. Correlation ID shall be unique within an AIOTF.

5.7.4 AIoT Device Temporary Identifier

A Device Temporary Identifier may be used as AIoT Identification Information in the Inventory procedure if privacy protection is used. The details of how the AIoT Device Temporary Identifier is generated, managed and used is specified in TS 33.369 [9].

5.8 Filtering Information

The Filtering Information is used to identify or filter one or multiple AIoT Device(s). The Filtering Information is constructed by one or multiple filtering elements and each filtering element corresponds to a component (i.e. ID Type, PLMN Identifier, NID, Third Party Identifier or Identification Information) of the AIoT Device Permanent Identifier as defined in clause 5.7.

Each filtering element shall include:

- Component Type Information indicating a component of the AIoT Device Permanent Identifier that is used to match the bitstring.
- A bitstring which is used to compare with the component.
- An Offset from the beginning of the indicated component of the AIoT Device Permanent Identifier, which indicates the start location in the indicated component to be used to compare with the corresponding bitstring.
- A Length indicating the length of the bitstring.

When the Component Type Information of a filtering element indicates a PLMN ID, NID or Third-Party Identifier component, then the Offset and Length are not included in the filtering element, i.e. the whole component is compared with the bitstring.

When the Component Type Information of the filtering element indicates an Identification Information or ID Type component, the Offset and Length are always included and the indicated component is compared from the start location indicated by the Offset with the bitstring for its entire indicated Length. The AIOTF includes at most one filtering element within the Filtering Information for the ID Type, PLMN ID, NID and Third Party Identifier components of the AIoT Device Permanent Identifier.

There may be multiple filtering elements corresponding to the component Identification Information of the AIoT Device Permanent Identifier.

NOTE 1: It is assumed that the AIoT Device does not validate the number of filtering element(s) for any indicated component within the Filtering Information.

NOTE 2: The format of the Filtering Information is specified in clause 31.3 of TS 23.003 [6].

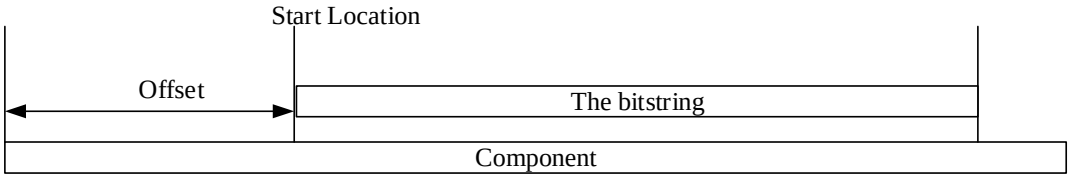


Figure 5.8-1: The example of the comparing the bitstring to the component

To determine whether an AIoT Device Permanent Identifier matches the Filtering Information, the bitstring of every filtering element within the Filtering Information is compared with the indicated component of the AIoT Device Permanent Identifier. If all the compared bitstrings match the corresponding component of the AIoT Device Permanent Identifier, then an AIoT Device Permanent Identifier matches the Filtering Information. If an AIoT Device Permanent Identifier does not contain an indicated component then it does not match the Filtering Information.

5.9 AIoT Service Operation Result Aggregation

An AIoT service operation may involve many AIoT Devices. The NG-RAN may perform AIoT service operation result aggregation with a specific Correlation ID based on the aggregation assistance information received from the AIOTF for a service operation request as specified in clause 5.4.

The AIOTF determines the aggregation assistance information based on the request from the AF or local configuration, which includes:

- Time interval: the fixed time interval for which NG-RAN collects multiple AIoT Devices' operation responses before reporting the aggregated AIoT response to the AIOTF. The reporting based on time interval may potentially happen multiple times until the NG-RAN completes the request operation.

If the AF has provided a time interval, then the AIOTF should signal a time interval to the NG-RAN that is equal or shorter than the time interval received from the AF.

NOTE: Based on local configuration, the AIOTF can reject the AF request, e.g. if the AF provided time interval is shorter than a locally configured minimum interval.

If the AIOTF does not provide aggregation assistance information, the aggregation process in the NG-RAN may be determined by implementation.

The AIOTF may also aggregate the results of a requested service operation before sending them to the NEF or trusted AF.

5.10 AIoT Device Location

5.10.1 Overview

During an inventory procedure (see clause 6.2.2) or a command procedure (see clause 6.2.3), the AIOTF may be requested to report AIoT Device Locations. Based on operator policy, the AIOTF determines whether to provide the AIoT Device location to the AF.

The Inventory Report(s) sent by NG-RAN include a RAN Reader ID for each reported AIoT Device. The location of each RAN Reader may be configured in the AIOTF. If configured, the AIOTF uses the location of RAN Reader to determine the location of the AIoT Device.

NOTE: The location format is defined based on the SLA between the operator and the AF, which is out the scope of 3GPP.

5.11 AIoT Device Context in AIOTF

The AIOTF supports management of the AIoT Device context information locally. The AIoT Device context includes e.g. the AIoT Device Permanent Identifier, the last known RAN Reader information, RAN AIoT Device NGAP ID, etc.

The last known RAN Reader information can be used to support the AIOTF to perform RAN Reader selection as defined in clause 5.3.3.

Table 5.11-1 below describes information storage structures for AIoT Device context.

Table 5.11-1: AIoT Device Context in AIOTF

Field	Description
AIoT Device Permanent Identifier	Uniquely identifies the AIoT Device.
Last known RAN Reader information	Indicate the last known RAN Reader that serves the AIoT Device.
RAN AIoT Device NGAP ID	Indicate the RAN AIoT Device NGAP ID used to transfer the NGAP AIoT Command messages towards the AIoT Device between AIOTF and NG-RAN.

NOTE: When to erase the stored AIoT Device context is up to implementation and local configuration.

6 AIoT Procedures

6.1 General

Clause 6.2 describes the AIoT procedures and Network Function services for the 5GS by end-to-end information flows and making use of the NF service operations defined in clause 7, in those information flows.

6.2 AIoT Service Procedures

6.2.1 General

Clause 6.2.2 provides the procedure for AIoT Inventory. Clause 6.2.3 provides the procedure for AIoT Command. Clause 6.2.5 provides the AIoT Session release procedure for AIoT Inventory and AIoT Command.

The AIOTF may perform the procedure in Clause 6.2.2 or Clause 6.2.3 for the resynchronization of T-ID as specified in clause 5.4.4 of TS 33.369 [9].

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.

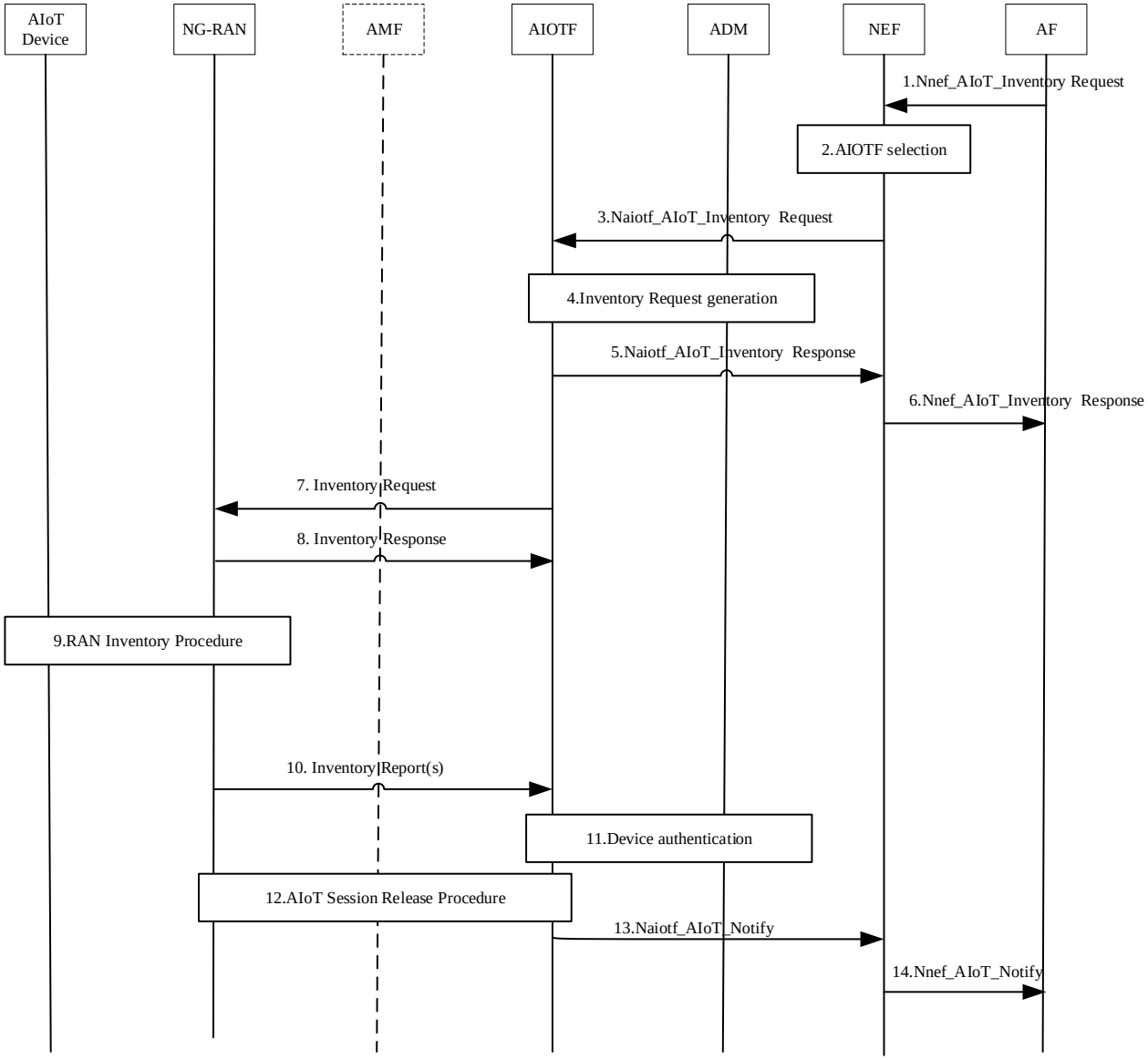


Figure 6.2.2-1: Inventory Procedure

1. The AF invokes Nnef_AIoT_Inventory Request (AF ID, [External Target Area information], [information about the target AIoT Device(s)], [Approximate number of AIoT Devices], [time interval], [location information requested]) 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). If Information about the target AIoT Device(s) is not included, the Inventory Request is for all AIoT Devices.

   The Approximate number of AIoT Devices, if provided, is used to determine the number of AIoT Devices expected to respond to this inventory AIoT service operation request, 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.

   The location information requested parameter indicates whether the AF expects the network to provide AIoT Device location information.

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. If no AIOTF can be selected, the NEF

rejects the Nnef_AIoT_Inventory request with an appropriate cause code and step 6 is performed before ending the procedure.

3. The NEF invokes the Naiotf_AIoT_Inventory Request (AF ID, [Target Area information], [information about the target AIoT Device(s)], [Approximate number of AIoT Devices], [time interval], [location information requested]) towards each of the selected AIOTF(s).

4. The AIOTF receives the Naiotf_AIoT_Inventory 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 is skipped.

   The AIOTF generates a Correlation ID corresponding to this AIoT service operation request and the Correlation ID is used for the AIOTF to correlate the service operation responses received from NG-RAN to the AIOTF request. The AIOTF creates the AIoT Session for the AF service operation request, which is identified by the Correlation ID.

   The AIOTF obtains security parameters from the ADM, as described in TS 33.369 [9].

   If the information about the target AIoT Device(s) received in step 1 is AIoT Device Permanent Identifier(s), and privacy protection is used, the AIOTF retrieves the AIoT Device Temporary Identifier and temporary identifier related information for each target AIoT Device from the ADM as described in TS 33.369 [9].

   The AIoT Identification Information to be provided to NG-RAN contains either Filtering Information as defined in clause 5.8, an AIoT Device Permanent Identifier as defined in clause 5.7.2 or an AIoT Device Temporary Identifier as defined in clause 5.7.4.

NOTE 1: The structure of AIoT Identification Information is defined in TS 23.003 [6].

   If no AIoT Identification Information is provided to NG-RAN, then the NG-RAN inventories all AIoT Devices.

NOTE 2: The concerns of paging all or paging a large group of AIoT Devices are described in TS 33.369 [9].

   The AIoT Identification Information and security parameters are provided to NG-RAN in step 7.

   The AIOTF performs Reader Selection, see clause 5.3.3. If no NG-RAN or RAN Reader can be selected, the AIOTF rejects the AIoT service operation request with an appropriate cause code.

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

   The AIOTF may perform AMF selection as described in clause 5.3.4.

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

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

7. The AIOTF sends the Inventory Request message including AIoT Identification Information and security parameters determined in step 4 to be included in the paging message, Correlation ID, Requested Service Area Information and assistance information to the selected NG-RAN node(s) 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 it will perform the AIoT service operation as specified in TS 38.413 [10]. If the Inventory Request is not rejected, then an AIoT Session is created in the NG-RAN. After this step, the AIoT Session between the NG-RAN and AIOTF, identified by Correlation ID, is established.

9. Upon reception of the Inventory Request message from the AIOTF, the RAN Reader(s) 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 and the security parameters.

   If the received AIoT Identification Information contains:

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

- AIoT Device Temporary Identifier, the AIoT Device determines whether it matches the AIoT Identification Information, as described TS 33.369 [9].

- AIoT Device Permanent Identifier, the AIoT Device determines whether it matches the AIoT Identification Information by comparing it with the stored AIoT Device Permanent Identifier.

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 Inventory Report that includes its device specific authentication information as specified in TS 33.369 [9] and optionally the AIoT Device Permanent Identifier if privacy protection is not used.

10. NG-RAN sends one or more Inventory Report messages to the AIOTF including the Correlation ID, Reader ID and the AIoT NAS Inventory Report(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) as part of the AIoT Device context.

    When the NG-RAN detects that no more AIoT Devices will respond to the inventory procedure, the NG-RAN informs the AIOTF by including the Inventory Complete Indication in the last Inventory Report message.

11. The AIOTF authenticates the AIoT Device and obtains the AIoT Device Permanent Identifier as specified in TS 33.369 [9]. The AIOTF may aggregate the results.

12. If the NG-RAN has sent an inventory complete indication in step 10, the AIOTF triggers the AIoT Session Release procedure defined in clause 6.2.5 to release the AIoT Session between the NG-RAN and the AIOTF.

13. The AIOTF reports the progress of the Naiotf_AIoT_Inventory request to the NEF by sending the Naiotf_AIoT_Notify message including a list of AIoT Device Permanent Identifier(s) and optionally location of each AIoT Device. The AIOTF may send multiple reports.

    Based on operator policy, if the location information is requested by the AF and if the location of the RAN Reader is configured, the AIOTF uses the Reader ID reported from NG-RAN in step 10 to determine the AIoT Device location.

    The AIOTF in the final Naiotf_AIoT_Notify message indicates it is the last report for this operation. The final Naiotf_AIoT_Notify message with the Last Report Indication is sent when all the involved NG-RAN nodes have completed the inventory procedure. When the last report is sent, the AIOTF ends the AIoT Session. If multiple AIOTFs are involved in the procedure, the NEF may receive Naiotf_AIoT_Notify messages from multiple AIOTFs.

14. When receiving the Naiotf_AIoT_Notify message from an AIOTF, the NEF informs the AF of the outcome of the Nnef_AIoT_Inventory request by sending the Nnef_AIoT_Notify message(s) including the AIoT Device Permanent Identifier(s) and optionally the location of each AIoT Device. The NEF in the final Nnef_AIoT_Notify message indicates that it is the last report for this operation.

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.

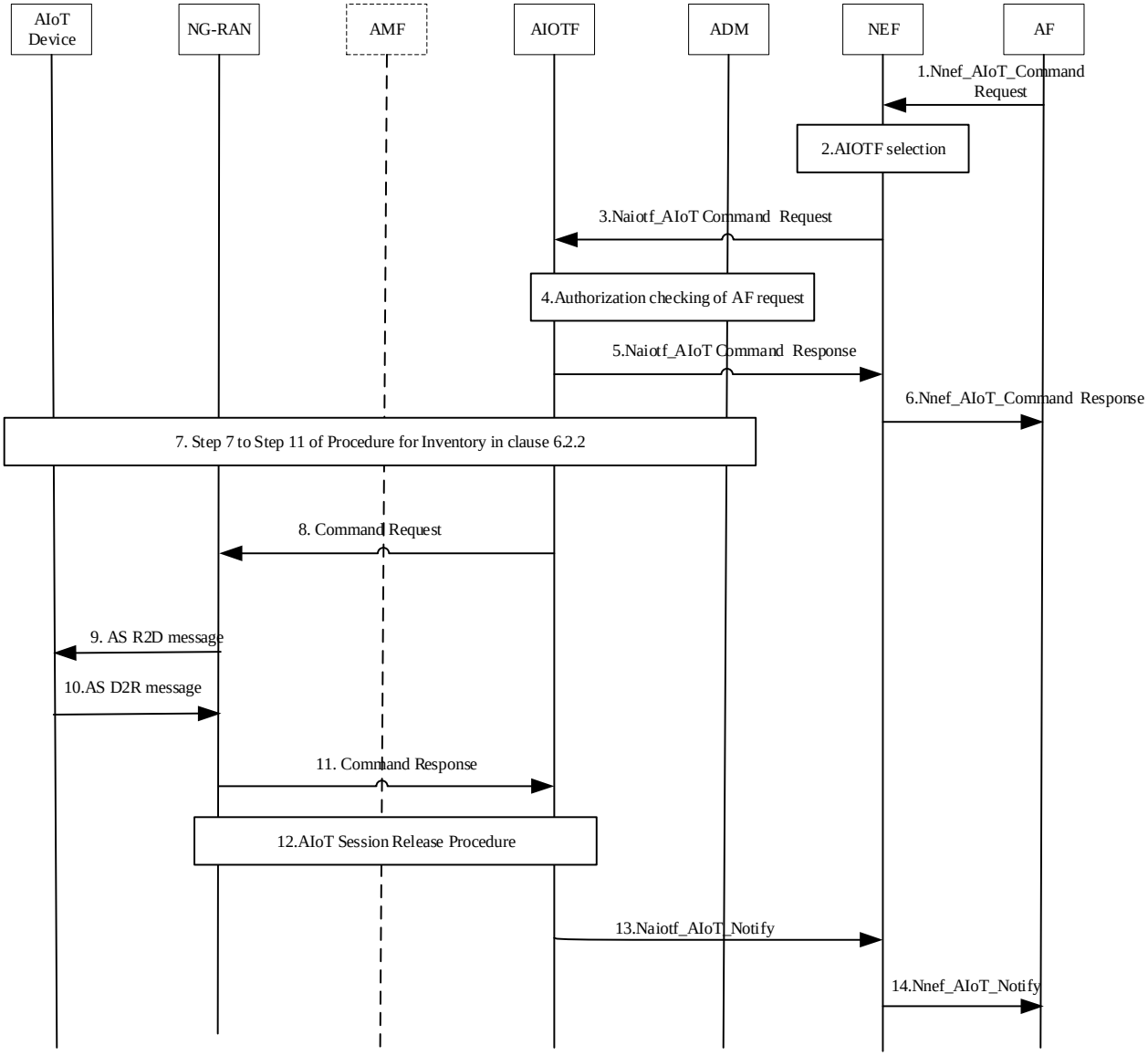


Figure 6.2.3-1: Command Procedure

1. The AF sends the Nnef_AIoT_Command Request message (AF ID, Command Type, [information about the target AIoT Device(s)], [External Target Area information], [Approximate number of AIoT Devices], [Command type specific parameters], [location information requested]) 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 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 AIoT service operation request, 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 Command service operations are described in clause 5.2.2.

   The location information requested parameter indicates whether the AF expects the network to provide AIoT Device location information.

2. Step 2 of the inventory procedure specified in clause 6.2.2 is performed for External Target Area information processing and AIOTF selection with the following clarifications:

- If AIOTF selection fails, the NEF rejects the Nnef_AIoT_Command request with an appropriate cause code and step 6 of this procedure 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], [Command type specific parameters], [location information requested]) message to the selected AIOTF(s).

4. The AIOTF receives the Naiotf_AIoT_Command Request and checks the parameters included in the request. The AIOTF performs Reader Selection as specified in clause 5.3.3. If no NG-RAN or RAN Reader can be selected, the AIOTF rejects the AIoT service operation request with an appropriate cause code and step 7 onward is skipped.

   The AIOTF generates a Correlation ID corresponding to this AIoT service operation request and the Correlation ID is used for the AIOTF to correlate the service operation responses received from NG-RAN to the request. The AIOTF creates the AIoT Session for the AF service operation request, which is identified by the Correlation ID.

   The AIOTF retrieves security parameters from the ADM, as described in TS 33.369 [9], and provides them to the NG-RAN in step 7.

   The AIOTF performs Reader Selection, see clause 5.3.3. If no NG-RAN or RAN Reader can be selected, the AIOTF rejects the AIoT service operation request with an appropriate cause code.

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

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

   If the information about the target AIoT Device(s) received in step 1 is AIoT Device Permanent Identifier(s), and privacy protection is used, the AIOTF retrieves the AIoT Device Temporary Identifier and temporary identifier related information for each target AIoT device from the ADM as described in TS 33.369 [9]. The AIoT Device Temporary Identifier(s) and related information is then to be used as the AIoT Identification Information in step 7.

   The AIOTF may perform 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 step 11 of the inventory procedure 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 authenticates the AIoT Devices as specified in TS 33.369 [9], and determines whether the command should be sent to an AIoT Device, e.g., by checking the information about the target AIoT Device(s). The AIOTF updates the corresponding AIoT Device contexts in the AIOTF to include the RAN AIoT Device NGAP ID.

If no successful AIoT NAS Inventory Report is received, step 8 to step 11 are not performed and the AIOTF sends a failure report to the NEF in step 12.

8. For each successful AIoT NAS Inventory Report received, the AIOTF sends Command Request message (Correlation ID, [Reader ID], AIoT NAS Command Request, Size of the Command Response message from the AIoT Device, RAN AIoT Device NGAP ID) included in NGAP AIoT information to NG-RAN for each AIoT Device. The AIoT NAS Command Request message includes the AIoT data. The Correlation ID is the same Correlation ID as generated in step 4. The RAN AIoT Device NGAP ID 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 AIoT NAS Command Request to send to the AIoT Device, as described in clause 5.2.2.

   The protection of the AIoT NAS Command Request message is specified in clause 5.3 of TS 33.369 [9].

NOTE 1: Command Request messages can be sent to NG-RAN when inventory procedure is ongoing.

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

10. The AIoT Device performs security checks on the received AIoT NAS Command Request and sends an AS message (including the AIoT 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 AIoT NAS Command Response message is specified in clause 5.3 of TS 33.369 [9].

11. The NG-RAN responds with a Command Response message (Correlation ID, Reader ID, AIoT NAS Command Response, RAN AIoT Device NGAP ID) included in NGAP AIoT information to the AIOTF. The AIOTF determines the AIoT Device context by the RAN AIoT Device NGAP ID received.

    If the AIoT NAS Command Response indicates the Command Type is not supported by the AIoT Device, the AIOTF reports the error result in step 13 and step 14.

NOTE 2: The AIOTF can take this into account to avoid initiating further command procedures of the same Command Type towards the AIoT Device by implementation.

    If the Command Type is "Permanent Disable" and the AIoT NAS Command is successful, the AIOTF should remove the Last known RAN Reader information from the AIoT Device Context in AIOTF.

12. After receiving the inventory complete indication in the last inventory report from the NG-RAN, when the AIOTF has completed sending Command Requests and the Command Responses have been received, the AIOTF initiates the AIoT Session Release Procedure in clause 6.2.5 to release the AIoT Session created during the inventory procedure.

13. The AIOTF reports the results of the Naiotf_AIoT_Command request to the NEF by sending Naiotf_AIoT_Notify message(s) (a list of AIoT Device(s) response information (AIoT Device ID(s), AIoT data and optionally location of each AIoT Device), AF ID, [Last Report Indication]). The AIOTF includes the Last Report Indication in the final Naiotf_AIoT_Notify message when all the involved NG-RAN nodes have completed the command procedure. If multiple AIOTFs are involved in the procedure, the NEF may receive Naiotf_AIoT_Notify messages from multiple AIOTFs.

    Based on operator policy, if the location information is requested by the AF and if the location of the RAN Reader is configured, the AIOTF uses the Reader ID reported from NG-RAN during the inventory procedure in step 7 to determine the AIoT Device location.

    When the last report is sent, the AIOTF ends the AIoT Session.

14. The NEF informs the AF of the result of the Nnef_AIoT_Command request by sending Nnef_AIoT_Notify message(s) (a list of AIoT Device(s) response information (AIoT Device ID(s), AIoT data and optionally location of each AIoT Device), AF ID, [Last Report Indication]).

6.2.4 Procedures between AIOTF and NG-RAN for Indirect Connectivity

6.2.4.1 Overview

An AIOTF and NG-RAN can use an indirect interface via an AMF as described in clause 4.2.2.4. The procedure for NGAP message delivery to NG-RAN is defined in clause 6.2.4.2 and the procedure for message delivery from NG-RAN is defined in clause 6.2.4.3.

6.2.4.2 Message delivery to NG-RAN

When the AIOTF sends an NGAP message, the AMF receives an Namf_AIoT_MessageDelivery request and sends the corresponding NGAP message to NG-RAN. The additional steps used for an indirect interface from an AIOTF to NG-RAN are shown in Figure 6.2.4.2-1.

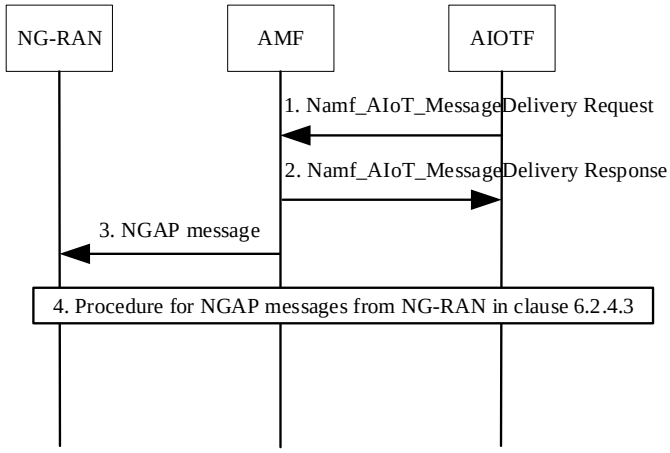


Figure 6.2.4.2-1: Procedure for NGAP message delivery to NG-RAN using indirect connectivity via an AMF

1. The AIOTF sends Namf_AIoT_MessageDelivery Request message (NGAP AIoT information, NG-RAN ID, AIOTF ID, Correlation ID, AIoT NGAP Message Type, Notification endpoint, [RAN AIoT Device NGAP ID]) to the AMF.

   The AIoT NGAP Message Type identifies the NGAP message to send to NG-RAN and NGAP AIoT information is provided to NG-RAN in the NGAP message. The message includes RAN AIoT Device NGAP ID if the AIoT NGAP Message Type indicates "Command Request".

2. The AMF responds to the AIOTF with a result indicating whether the AMF will handle the request. If a failure is indicated by the result indication, then the procedure stops and the remaining steps are skipped.

   If the AMF accepts the request, the AMF maintains a context for the transaction including the NG-RAN ID, AIOTF ID, Correlation ID, RAN AIoT Device NGAP ID (if received) and Notification endpoint. This context is used to route multiple NGAP messages from NG-RAN to AIOTF, see clause 6.2.4.3. The AIOTF is implicitly subscribed to Namf_AIoT_Notify events.

3. The AMF sends an NGAP message (AIOTF ID, Correlation ID, NGAP AIoT information, [RAN AIoT Device NGAP ID]) to the target NG-RAN.

4. The procedure for handling NGAP messages from NG-RAN is used to route NGAP messages from NG-RAN to the AIOTF, see clause 6.2.4.3.

6.2.4.3 Message delivery to AIOTF

When the AMF receives an NGAP message from NG-RAN, for example, responses to a procedure or events like Inventory Reports, the AMF determines which AIOTF to send a Namf_AIoT_Notify to and sends the information from NG-RAN to that AIOTF. The additional steps used for an indirect interface from NG-RAN towards an AIOTF is shown in Figure 6.2.4.3-1.

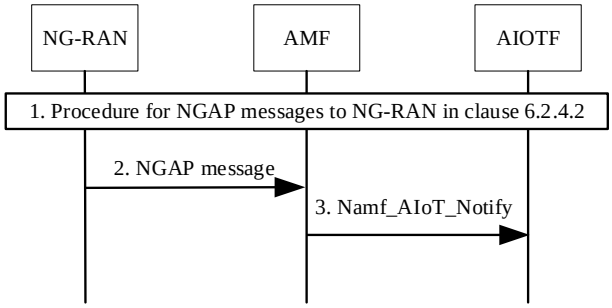


Figure 6.2.4.3-1: Procedure for NG-RAN event handling using indirect connectivity via an AMF

1. Before any NGAP messages can be routed from NG-RAN to the AIOTF, the AMF needs routing information to be able to route them, see clause 6.2.4.2. The same context created in clause 6.2.4.2 includes such routing information and can be used to route multiple NGAP messages from NG-RAN.

2. NG-RAN sends an NGAP message (AIOTF ID, Correlation ID, NGAP AIoT information, [RAN AIoT Device NGAP ID]) to an AMF. NGAP AIoT information is determined by NG-RAN depending upon the operation the NGAP message relates to.

3. AMF determines the Notification endpoint from the context using the AIOTF ID, the Correlation ID, the NG-RAN ID and optionally the RAN AIoT Device NGAP ID received in step 2 from NG-RAN, and then sends the Namf_AIoT_Notify message (AIoT NGAP Message Type, NGAP AIoT information) to the AIOTF.

   Step 2 and step 3 are repeated for each NGAP message received from NG-RAN.

   If the message received from NG-RAN is an Inventory Failure indicating an error or an AIOT Session Release Complete, then the AMF releases the context which is associated with the NG-RAN ID, the AIOTF ID and the Correlation ID, after sending the Namf_AIoT_Notify message to the AIOTF.

6.2.5 AIoT Session Release Procedure

This procedure is used to release the AIoT Session between the NG-RAN and the AIOTF. The AIoT Session release procedure can be triggered by the AIOTF or the NG-RAN node and is specified in TS 38.413 [10].

The initiation of AIoT Session release may be:

- NG-RAN-initiated e.g. if the NG-RAN detects no AIoT Devices responds to the inventory procedure or the command procedure; or

- AIOTF-initiated, e.g. if the AIOTF fails validating the results of AIoT NAS Inventory Report as specified in TS 33.369 [9] in the command procedure.

Both NG-RAN-initiated and AIOTF-initiated AIoT Session Release procedures are shown in Figure 6.2.5-1.

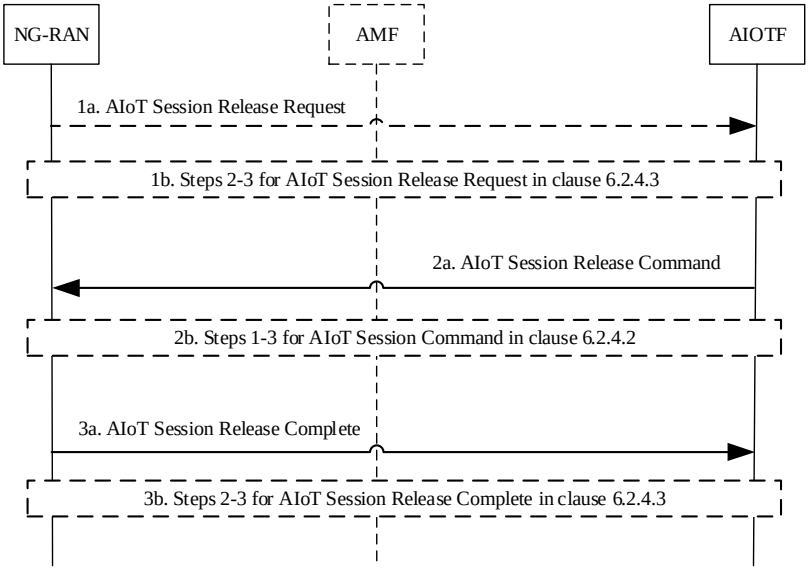


Figure 6.2.5-1: AIoT Session Release Procedure

1. NG-RAN may decide to initiate the AIoT Session release procedure. NG-RAN sends an AIoT Session Release Request message (Correlation ID, Cause) to the AIOTF directly (step 1a) or performs steps 2-3 of Message delivery to AIOTF specified in clause 6.2.4.3 (step 1b) when the indirect interface between an AIOTF and NG-RAN is used.

2. If the AIOTF receives the AIoT Session Release request message or the AIOTF decides to terminate all activities related to the AIoT Session, the AIOTF sends an AIoT Session Release Command message (Correlation ID, Cause) to the NG-RAN directly (step 2a) or performs steps 1-3 of Message delivery to NG-RAN specified in clause 6.2.4.2 (step 2b) when the indirect interface between an AIOTF and NG-RAN is used.

3. The NG-RAN node releases the AIoT Session and radio resources related to the AIoT session identified by the Correlation ID provided by the AIOTF, as specified in TS 38.300 [5]. The NG-RAN confirms the AIoT Session Release by sending an AIoT Session Release Complete message (Correlation ID) to the AIOTF directly (step 3a) or performs steps 2-3 of Message delivery to AIOTF specified in clause 6.2.4.3 (step 3b) when the indirect interface between an AIOTF and NG-RAN is used. The AIOTF releases AIoT Session.

7 Network Functions Services

7.1 General

The following clauses provide for each involved NF the NF services it exposes through its service-based interfaces for AIoT Services.

7.2 AIOTF services

7.2.1 General

The AIOTF supports to expose AIoT services towards the AF or the NEF as described in Table 7.2.1-1.

Table 7.2.1-1: NF services provided by the AIOTF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Naiotf_AIoT	Inventory	Request/Response	NEF, AF
	Command	Request/Response	NEF, AF
	Notify	Subscribe/Notify	NEF, AF

7.2.2 Naiotf_AIoT_Inventory service operation

Service operation name: Naiotf_AIoT_Inventory.

Description: The NF consumer requests an inventory AIoT service operation for one or multiple AIoT Device(s).

Inputs, Required:

- AF ID.
- At least one of the following parameters are included:
  - Target Area information for the inventory operation.
  - Information about the target AIoT Device(s):
    - Either the AIoT Device ID(s) or Filtering Information (see clause 5.8) for multiple target AIoT Devices.
- Notification Target Address and the Notification Correlation ID.

Inputs, Optional:

- Information to be used for resource allocation:
  - Approximate number of AIoT Devices.
- Time Interval for result aggregation.
- Location information requested.

Outputs, Required: Subscription Correlation ID, Result indication (Success or Failure), Failure Cause in case of Failure.

Outputs, Optional: None.

7.2.3 Naiotf_AIoT_Command service operation

Service operation name: Naiotf_AIoT_Command.

Description: The NF consumer requests a Command AIoT service operation for one or multiple AIoT Device(s).

Inputs, Required:

- AF ID.
- At least one of the following parameters are included:
  - Target Area information for the command operation.
  - Information about the target AIoT Device(s):
    - either the AIoT Device ID(s) or the filtering information (see clause 5.8) for multiple AIoT Devices.
- Notification Target Address and the Notification Correlation ID.
- Command Type: Read, Write or Permanent Disable.

Inputs, Optional:

Information to be used for resource allocation:

- Approximate number of AIoT Devices.

- If the Command Type is Read, the offset to read application data from and the length of application data to read shall be included.
- If the Command Type is Write, the offset where to write the application data, the application data to write and its length shall be included.
- Location information requested.

Outputs, Required: Subscription Correlation ID, Result indication (Success or Failure), Failure Cause in case of Failure.

Outputs, Optional: None.

7.2.4 Naiotf_AIoT_Notify service operation

Service operation name: Naiotf_AIoT_Notify

Description: The AIOTF uses this service operation to notify the results or status of the AIoT service operation towards the NF consumers. If the NF consumer invokes the Naiotf_AIoT_Inventory, or Naiotf_AIoT_Command service operation, the NF consumer implicitly subscribes to the results of the requested service operation.

Inputs, Required:

- Common report information: Notification Correlation ID.

Inputs, Optional:

- List of Notification information with zero or more entries, each of which includes the following contents:
  - AIoT Device ID;
  - Result indication (Success or Failure), Failure Cause in case of Failure;
  - Specific report information obtained from target AIoT Device for Read command;
  - Location information of each AIoT Device.
- The Last Report Indication, indicating the notify is the last notify for the AIoT service operation.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.3 AMF services

7.3.1 General

AMF supports to expose AIoT services towards the AIOTF as described in Table 7.3.1-1. The Namf_AIoT AMF service is used when the NG-RAN and the AIOTF communicate indirectly via an AMF.

Table 7.3.1-1: NF services provided by the AMF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Namf_AIoT	MessageDelivery	Request/Response	AIOTF
	Notify	Subscribe/Notify	AIOTF

7.3.2 Namf_AIoT_MessageDelivery service operation

Service operation name: Namf_AIoT_MessageDelivery

Description: The NF consumer requests to send AIoT NGAP Messages towards NG-RAN.

Inputs, Required:

- NGAP AIoT Information to deliver to NG-RAN.
- NG-RAN ID.
- AIoT NGAP Message Type ("Inventory Request" or "Command Request" or "Session Release Command").
- AIOTF Identifier and Correlation ID, this is to allow identifying the association between NG-RAN and AMF.
- Notification Endpoint.

Outputs, Required: Result indication (Success or Failure), Failure Cause in case of Failure.

7.3.3 Namf_AIoT_Notify service operation

Service operation name: Namf_AIoT_Notify

Description: The NF consumer requests to receive notifications for AIoT NGAP messages from NG-RAN. If the NF consumer invokes the Namf_AIoT_MessageDelivery, the NF consumer implicitly subscribes to receive the Namf_AIoT_Notify.

Inputs, Required:

- AIoT Information received from NG-RAN.
- AIoT NGAP Message Type ("Inventory Response", "Inventory Failure", "Inventory Report", "Command Response", "Command Failure", "Session Release Complete").

Input, Optional: None.

Outputs, Required: Operation execution result indication.

Output, Optional: None.

7.4 NEF services

7.4.1 General

In addition to those defined in clause 7.2.8 of TS 23.501 [3] and clause 5.2.6 of TS 23.502 [4], table 7.4.1-1 illustrates additional NEF services to support AIoT.

Table 7.4.1-1: NF Services provided by NEF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnef_AIoT	Inventory	Request/Response	AF
	Command	Request/Response	AF
	Notify	Subscribe/Notify	AF

7.4.2 Nnef_AIoT_Inventory service operation

Service operation name: Nnef_AIoT_Inventory

Description: The consumer requests to perform an inventory AIoT service operation for one or multiple AIoT Device(s).

Input, Required:

- AF ID.
- At least one of the following parameters are included:
  - External Target Area information.
  - Information about the target AIoT Device(s):
  - Either AIoT Device ID(s) or Filter Information (see clause 5.8) for multiple target AIoT Devices.
- Notification Target Address and Notification Correlation ID.

Input, Optional: Approximate number of AIoT Devices, time interval, location information requested.

Output, Required: Subscription Correlation ID, Result indication, Failure cause in case of Failure.

Output, Optional: None.

7.4.3 Nnef_AIoT_Command service operation

Service operation name: Nnef_AIoT_Command

Description: The consumer requests to perform a command AIoT service operation for one or multiple AIoT Device(s).

Input, Required:

- AF ID.
- At least one of the following parameters are included:
  - External Target Area information.
  - Information about the target AIoT Device(s):
    - Either AIoT Device ID(s) or Filter Information (see clause 5.8) for multiple AIoT Devices.
- Notification Target Address and Notification Correlation ID.
- Command type (Read, Write, or Permanent Disable).

Input, Optional: Approximate number of AIoT Devices, if the Command Type is Read, the offset to read application data from and the length of application data to read shall be included, if the Command Type is Write the offset where to write the application data, the application data to write and its length shall be included, location information requested.

Output, Required: Subscription Correlation ID, Result indication, Failure cause in case of Failure.

Output, Optional: None.

7.4.4 Nnef_AIoT_Notify service operation

Service operation name: Nnef_AIoT_Notify

Description: The consumer receives notification of the status or results of the requested AIoT service operation. If the consumer invokes the Nnef_AIoT_Inventory, or Nnef_AIoT_Command service operation, the consumer implicitly subscribes to the results of the requested service operation.

Input, Required:

- Notification Correlation ID.

Input, Optional:

- a list of Notification information with zero or more entries, each of them includes the following contents:
  - AIoT Device ID(s);
  - Result indication (Success or Failure), Failure Cause in case of Failure;
  - Specific report information obtained from target AIoT Device for Read command;
  - Location information of each AIoT Device.
- The Last Report Indication, indicating the notify is the last notify for the AIoT service operation.

Output, Required: Result indication.

Output, Optional: None.

7.5 ADM services

7.5.1 General

The following table shows the Nadm_DM Service and Service Operations.

Table 7.5.1-1: NF services provided by ADM

NF service name	Service Operations	Operation Semantics	Example Consumer(s)
Nadm_DM	Query	Request/Response	AIOTF, NEF
	Update	Request/Response	AIOTF
	Subscribe	Subscribe/Notify	AIOTF
	Unsubscribe		AIOTF
	Notify		AIOTF

7.5.2 Nadm_DM_Query service operation

Service operation name: Nadm_DM_Query

Description: NF service consumer may request the AIoT Device Profile Data or the AF authorization data from the ADM.

Inputs, Required: AIoT Device Permanent Identifier (if retrieving AIoT Device Profile Data), AF ID (if retrieving a specific AF's authorization data; if not provided, all AFs' authorization data are retrieved).

Input, Optional: None.

Outputs, Required: the AIoT Device Profile Data or the AF authorization data.

Output, Optional: None.

7.5.3 Nadm_DM_Update service operation

Service operation name: Nadm_DM_Update

Description: NF service consumer may update the AIoT Device Profile Data in the ADM.

Inputs, Required: AIoT Device Permanent Identifier, updated AIoT Device Profile Data.

Input, Optional: None.

Outputs, Required: Result indication (Success or Failure), Failure Cause in case of Failure.

Output, Optional: None.

7.5.4 Nadm_DM_Subscribe service operation

Service operation name: Nadm_DM_Subscribe

Description: NF service consumer performs the subscription to notifications to data modified in the ADM. The events can be changes on existing data, addition of data. Specifically, this service operation together with the corresponding Unsubscribe and Notify service operations are used by the AIOTF to manage notifications of changes of AF authorization data in ADM.

Inputs, Required: Requested AIoT data type (only for AF authorization data), Notification Target Address and Notification Correlation ID.

Inputs, Optional: AF ID, Subscription Correlation ID (in the case of modification of the subscription).

Outputs, Required: When the subscription is accepted: Subscription Correlation ID.

Outputs, Optional: None.

7.5.5 Nadm_DM_Unsubscribe service operation

Service operation name: Nadm_DM_Unsubscribe

Description: NF service consumer unsubscribes from the notifications about data modified in the ADM. The events can be changes on existing data, addition of data.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Result.

Outputs, Optional: None.

7.5.6 Nadm_DM_Notify service operation

Service operation name: Nadm_DM_Notify

Description: ADM notifies NF service consumer(s) about modification of data, when data in the ADM is added, modified or deleted and an NF needs to be informed about this, due to a previous subscription to notifications procedure with the ADM.

Inputs, Required: Notification Correlation ID, Updated Data.

Inputs, Optional: None.

Outputs, Required: Result.

Outputs, Optional: None.

7.6 UDR Services

7.6.1 Nudr_DataManagement (DM) Service

7.6.1.1 General

The ADM makes use of the Nudr_DM service for Ambient IoT Data, as described in clause 5.2.12 of TS 23.502 [4].

The Ambient IoT Data includes AIoT Device Profile Data and AF Authorization Data. The AIoT Device Permanent ID is the Data Key of AIoT Device Profile Data, while the AF ID is the Data Key of AF Authorization Data, as illustrated in Table 7.6.1.1-1.

Table 7.6.1.1-1: Data keys

Data Set	Data Subset	Data Key	Data Sub Key
Ambient IoT Data	AIoT Device Profile Data	AIoT Device Permanent Identifier	-
	AF Authorization Data	AF ID	-

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2025-01	SA2#166 AH-e	S2-2501256	-	-	-	Proposed skeleton agreed at SA2#166AH-e	0.0.0
2025-06	SP#108	SP-250489	-	-	-	MCC editorial update for presentation to TSG SA for approval	1.0.0
2025-06	SP#108	-	-	-	-	MCC editorial update for publication after TSG SA approval	19.0.0
2025-09	SP#109	SP-250948	0001	1	F	Removal of AIoT service type provided to NG-RAN	19.1.0
2025-09	SP#109	SP-250948	0005	2	B	Session release procedure and correlation ID	19.1.0
2025-09	SP#109	SP-250948	0007	2	B	Support of Device Location in Ambient IoT	19.1.0
2025-09	SP#109	SP-250948	0010	2	F	Nudr Service for Accessing AIoT Data	19.1.0
2025-09	SP#109	SP-250948	0043	1	F	Removal of EN for Device ID	19.1.0
2025-09	SP#109	SP-250948	0050	2	F	Term alignment and clarifications on AIOTF and Reader Selection	19.1.0
2025-09	SP#109	SP-250948	0054	2	F	Update of Procedures between AIOTF and NG-RAN for Indirect Connectivity	19.1.0
2025-09	SP#109	SP-250948	0063	2	F	Corrections to the Filtering Information	19.1.0
2025-09	SP#109	SP-250948	0065	3	F	Update to AIoT Area related	19.1.0
2025-09	SP#109	SP-251277	0068	1	F	Private Network Deployment Alignment	19.1.0
2025-12	SP#110	SP-251328	0029	5	F	Resolve Security Related ENs	19.2.0
2025-12	SP#110	SP-251328	0072	2	F	Update on Filtering Information	19.2.0
2025-12	SP#110	SP-251328	0078	1	F	Filtering Information security guidance	19.2.0
2025-12	SP#110	SP-251328	0084	1	F	Alignment for the security aspects	19.2.0
2025-12	SP#110	SP-251328	0085	2	F	Alignment related to completion and Session Release	19.2.0
2025-12	SP#110	SP-251328	0091	3	F	Security Alignment and Resolve ENs	19.2.0
2025-12	SP#110	SP-251328	0092	3	F	Handling of Unsupported Command	19.2.0
2025-12	SP#110	SP-251328	0096	2	F	Clarification on AmbientIoT Device	19.2.0
2025-12	SP#110	SP-251328	0101	7	B	Updates to AIOTF and ADM to support temporary ID	19.2.0
2025-12	SP#110	SP-251328	0103	2	F	Temporary Device ID description	19.2.0
2025-12	SP#110	SP-251328	0106	8	F	Update to Inventory procedure for use of Temporary Device ID	19.2.0
2025-12	SP#110	SP-251328	0109	2	F	Support of AIoT device context management	19.2.0
2025-12	SP#110	SP-251328	0123	2	F	Clarification on AIOT Device Profile Data and AIoT Security Data	19.2.0
2025-12	SP#110	SP-251328	0134	1	F	Update on AIoT Permanent ID Length	19.2.0
2026-03	SP#111	SP-260082	0011	4	F	ADM Service Operations Update	19.3.0
2026-03	SP#111	SP-260082	0090	4	F	Clarification on NG-RAN Configuration Information	19.3.0
2026-03	SP#111	SP-260082	0110	5	F	AMF service operations and procedures update	19.3.0
2026-03	SP#111	SP-260082	0140	2	F	Correction on AIOTF services	19.3.0
2026-03	SP#111	SP-260082	0142	1	D	Editorial correction on terms and update on general clause	19.3.0
2026-03	SP#111	SP-260082	0143	2	F	Clarification on AIoT Procedures	19.3.0
2026-03	SP#111	SP-260082	0144	1	F	Update on interaction between NG-RAN and AIOTF	19.3.0
2026-03	SP#111	SP-260082	0145	1	F	Update on length of Identification Information	19.3.0
2026-03	SP#111	SP-260082	0147	2	F	Update on the inventory and command procedure	19.3.0
2026-06	SP#112	SP-260430	0129	4	F	Clarification on determining of last report	19.4.0
2026-06	SP#112	SP-260430	0153	1	F	NEF Service Update to Align with AIOTF	19.4.0
2026-06	SP#112	SP-260430	0154	1	F	Corrections on Security Aspects in Inventory and Command Procedure	19.4.0
2026-06	SP#112	SP-260430	0175	-	F	Add reference to AIoT Identification Information structure	19.4.0
2026-06	SP#112	SP-260430	0198	3	D	Editorial clean-up, and term and descriptions alignments	19.4.0
2026-06	SP#112	SP-260430	0199	-	F	Correction to Read Response message size determination	19.4.0

History

Version	Date	Status
V19.1.0	January 2026	Publication
V19.2.0	February 2026	Publication
V19.3.0	March 2026	Publication
V19.4.0	July 2026	Publication