ETSI TS 124 369 V19.1.0 (2026-03)

TECHNICAL SPECIFICATION

5G;
Ambient IoT Non-Access-Stratum (AIoT NAS) protocol for 5G System (5GS);
Stage 3
(3GPP TS 24.369 version 19.1.0 Release 19)

Reference
RTS/TSGC-0124369vj10

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 the ambient internet of things (AIoT) non-access-stratum (NAS) protocol to support the transport of signalling and AIoT data between AIoT device and the AIoT function (AIOTF) in the 5G system (5GS) as specified in 3GPP TS 23.369 [2].

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

[2] 3GPP TS 23.369: "Architecture support for Ambient power-enabled Internet of Things; Stage 2".

[3] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[4] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[5] 3GPP TS 23.003: "Numbering, addressing and identification".

[6] 3GPP TS 33.369: "Security aspects of Ambient Internet of Things (AIoT) services for isolated private networks".

[7] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[8] 3GPP TS 38.391: "NR; Ambient IoT Medium Access Control Protocol specification".

[9] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.369 [2] apply:

AIoT Device

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

AIoT Ambient Internet of Things
AIOTF AIoT Function
MAC Message Authentication Code
NAS Non-Access-Stratum
T-ID Temporary Identifier

4 General

4.1 Overview

The AIoT NAS protocol described in the present document provides signalling between the AIoT device and the AIOTF, for 5GS. The AIoT NAS as part of the protocol stacks for support of AIoT services in 5GS is described in 3GPP TS 23.369 [2].

The main function of the AIoT NAS protocol is to support the AIoT procedures (see 3GPP TS 23.369 [2]):

a) inventory procedure; and

b) command procedure.

For the support of the above functions, the procedures are supplied within procedures for AIoT NAS, in clause 5.

The AIoT NAS messages are transported between the AIoT device and the AIOTF via AIOT1 reference point, and this transport does not involve N1 reference point. The AIoT NAS protocol specified in the present document is unrelated to the 5GMM NAS and 5GSM NAS protocols specified in 3GPP TS 24.501 [4].

Principles for the handling of AIoT NAS security, including ciphering and integrity protection of AIoT NAS messages, are provided in clause 4.2.

The AIoT NAS protocol for 5GS follows the protocol architecture model for layer 3 as described in 3GPP TS 24.007 [3].

4.2 AIoT NAS security

4.2.1 General

This clause describes the principles for the handling of AIoT security in the AIoT device and in the AIOTF and the procedures used for the security protection of AIoT NAS messages between AIoT device and AIOTF. AIoT NAS security includes authentication, AIoT NAS message security protection and AIoT device identifier privacy. AIoT NAS message security protection involves integrity protection and ciphering of the AIoT NAS messages.

When an AIoT NAS message needs to be sent both ciphered and integrity protected, the AIoT NAS message is first ciphered and then the ciphered AIoT NAS message is integrity protected by calculating the MAC.

The long-term credentials for authentication, integrity protection and ciphering are provisioned and stored in the AIoT device and in the network. The mechanism to provision and store long-term credentials is out of scope of 3GPP in this version of the present document. The relationship between the long-term credentials and security parameters is defined in 3GPP TS 33.369 [6].

The signalling procedures for the control of AIoT NAS security are part of the AIoT NAS protocol and are described in detail in clause 5.

4.2.2 Authentication

The authentication in Ambient IoT consists:

a) authentication of the AIoT device; and

b) authentication of the network.

Authentication of the AIoT device is done in the inventory procedure as specified in clause 5.2. A network generated $RAND_{AIOT\_n}$ is provided by the AIOTF and received by the AIoT device in the AIoT paging message. The $RAND_{AIOT\_n}$ value included in the AIoT paging message is provided to the AIoT NAS by lower layers. The AIoT device which is target of the AIoT paging (see clause 5.2.3), shall generate $RAND_{AIOT\_d}$, and use its AIoT device permanent identifier, the $RAND_{AIOT\_n}$, the generated $RAND_{AIOT\_d}$ and its long-term K_{AIOT_root} to derive a RES_{AIOT} as specified in 3GPP TS 33.369 [6]. The AIoT device shall include the RES_{AIOT} and the generated $RAND_{AIOT\_d}$ in the INVENTORY REPORT message to the AIOTF. The network shall verify the RES_{AIOT} to authenticate the AIoT device as specified in 3GPP TS 33.369 [6].

Upon successful verification, and when the AIOTF needs to initiate a command procedure as specified in clause 5.3 the AIOTF shall retrieve K_{AIOTF} and derive the integrity key $K_{Command\_int}$ to protect the AIoT NAS command message as described in 3GPP TS 33.369 [6]. When the AIoT device receives the AIoT NAS command message, it shall also derive the integrity key $K_{Command\_int}$ to verify the MAC and thereby implicitly authenticate the network, as described in 3GPP TS 33.369 [6].

The requirements for the AIoT device to derive RES_{AIOT} at receiving $RAND_{AIOT\_n}$ from lower layers are described in 3GPP TS 33.369 [6].

The requirements for parameters and algorithms used at AIoT authentication are specified in 3GPP TS 33.369 [6].

NOTE: The procedure parts for authentication as specified in 3GPP TS 33.369, clause 5.2.2, are specified in clause 5.2, Inventory procedure, and clause 5.3, Command procedures.

4.2.3 Integrity protection of AIoT NAS signalling messages

For the AIoT device and AIOTF, integrity protected signalling is applied for AIoT NAS messages. Integrity protection of all AIoT NAS signalling messages, except the INVENTORY REPORT message, is mandatory and the responsibility of the AIoT NAS.

The algorithm to calculate the integrity protection information is described in clause D.3 in 3GPP TS 33.501 [9], and the integrity protection shall include octets 1 and 6 to n of the security protected AIoT NAS messages. The AIoT NAS signalling message is integrity protected by calculating the message authentication code (MAC) using $K_{Command\_int}$ derived from K_{AIOTF} as specified in 3GPP TS 33.369 [6]. The calculated MAC shall be included in the MAC field (see clause 7.2.10).

In case of an AIoT NAS message fails the integrity check by the AIoT NAS, the AIoT device shall discard the AIoT NAS message and provide an indication to the lower layers that the AIoT NAS message was discarded due to integrity check failure.

In case of an AIoT NAS message fails the integrity check by the AIoT NAS, the AIOTF shall discard the AIoT NAS message.

4.2.4 Ciphering of AIoT NAS signalling messages

The use of ciphering in a network is an operator option subject to AIOTF configuration.

All AIoT NAS messages, except the INVENTORY REPORT message, shall be sent ciphered. The Security header IE is always unciphered in AIoT NAS messages according to 3GPP TS 33.369 [6].

The AIOTF indicates the selected ciphering algorithm in the Security header IE of the command message to the AIoT device.

When operation of the network without ciphering is configured, the AIOTF shall indicate "Integrity protected and ciphered with NEA0" in SPI field of the Security header IE as specified in clause 7.2.3. If the "null ciphering algorithm" NEA0 has been selected as a ciphering algorithm, the AIoT NAS message is regarded as ciphered.

The algorithm to calculate the ciphering of AIoT NAS messages is described in clause D.2 in 3GPP TS 33.501 [9], and the ciphered data shall include octets 6 to n of the security protected AIoT NAS messages. In addition to the data that is to be ciphered, the constant BEARER, DIRECTION bit, COUNT, KEY and LENGTH are input to the ciphering algorithm. These parameters are described in 3GPP TS 33.369 [6].

4.2.5 Privacy of AIoT device identifiers

The AIoT NAS protocol supports privacy of AIoT device identifiers by enabling the use of Temporary Identifiers (T-IDs), as specified in 3GPP TS 33.369 [6].

The network shall support that the mechanism for privacy protection and usage of privacy protection is based on the network policy and deployment.

The AIoT device shall support the mechanism for privacy protection and usage of privacy protection is determined by operator policy and is based on AIoT device's configuration.

When privacy protection is not used:

- the AIoT device permanent identifier is included as the AIoT identification information in the paging message for individual paging; and
- the AIoT device permanent identifier is included in the INVENTORY REPORT message sent as response to any paging message.

When privacy protection is used:

- T-ID is included as the AIoT identification information in the paging message for individual paging; and
- no AIoT device identity is included in the INVENTORY REPORT message sent as response to any paging message.

When T-ID is provided by the network in the paging message and privacy protection is used by the AIoT device, the AIoT device shall determine whether to respond based on a match between the received T-ID value and the local T-ID determined based on the T-ID type in the AIoT identification information provided by lower layers. The T-ID type indicates whether the T-ID is a:

- concealed T-ID; or
- stored T-ID.

If the T-ID type indicates a stored T-ID and upon successful match of the AIoT device locally stored T-ID and the received T-ID value, the locally stored T-ID is updated as determined based on the stored T-ID update indication. The stored T-ID update indication indicates either:

- update with command procedure; or
- update without command procedure.

If the stored T-ID update indication indicates "update with command procedure", the locally stored T-ID is replaced with the AIoT device T-ID IE value received in the subsequent AIoT NAS command message. If the stored T-ID update indication indicates "update without command procedure", the locally stored T-ID is replaced with a new T-ID value calculated as specified in 3GPP TS 33.369 [6], clause B.1.

5 Elementary procedures for AIoT NAS protocol

5.1 General

This clause describes the procedures used for AIoT NAS protocol performed between the AIoT device and the AIOTF. The format and coding of the messages and information elements are specified in clause 7.1 and 7.2 respectively.

The following AIoT NAS procedures can be distinguished:

a) procedure related to network initiated inventory request; and

b) procedure related to network initiated command request.

AIoT NAS messages are standard L3 messages according to 3GPP TS 24.007 [3] and error behaviour specified for L3 protocol according to 3GPP TS 24.007 [3] applies for AIoT unless otherwise specified in the present document.

The support of the read command procedure and the support of the write command procedure are optional for the AIoT device.

5.2 Inventory procedure

5.2.1 General

The inventory procedure is used to discover one or more AIoT devices:

a) if the AIoT identification information is not provided to NG-RAN, all the AIoT devices are to be discovered. In this case, an indication from lower layer is provided as specified in clause 5.2 of 3GPP TS 38.391 [8];

b) if the AIoT identification information is provided to NG-RAN and the AIoT identification information includes the filtering information, a group of AIoT devices that matches the AIoT identification information are to be discovered; and

c) if the AIoT identification information is provided to NG-RAN and the AIoT identification information includes an AIoT device identifier (see clause 4.2.5), a specific AIoT device that matches the AIoT identification information is to be discovered.

NOTE: Details of AIOTF providing the AIoT identification information to NG-RAN are defined in 3GPP TS 23.369 [2].

5.2.2 Inventory procedure initiation

To initiate the inventory procedure, the AIOTF sends an inventory request to the selected NG-RAN, as defined in 3GPP TS 38.413 [10]. The selected NG-RAN performs the AIoT paging by broadcast of the AIoT paging message that may include the AIoT identification information received in the inventory request (see 3GPP TS 38.300 [7] and 3GPP TS 38.391 [8]).

NOTE: How AIOTF selects NG-RAN is defined in 3GPP TS 23.369 [2].

Figure 5.2.2-1 gives an example of inventory procedure for an AIoT device which sends the INVENTORY REPORT message to AIOTF.

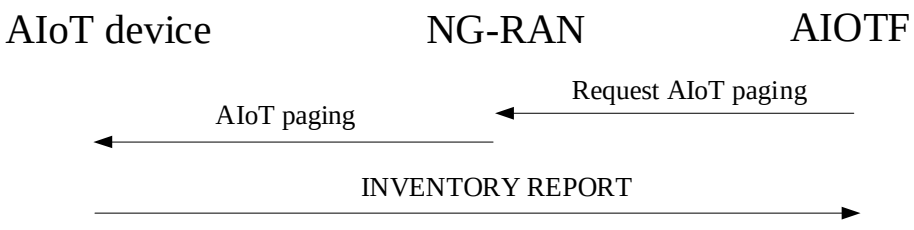

Figure 5.2.2-1: Inventory procedure

Upon receiving an AIoT paging message, the lower layers of the AIoT device determine whether to respond to the AIoT paging message as specified in 3GPP TS 38.391 [8]. The evaluation in lower layers includes interaction with upper layers to assess AIoT identification information as specified in clause 5.2.3, if the AIoT identification information is included in the AIoT paging message. If the AIoT identification information is not included in the AIoT paging message and lower layers determine to respond to the paging message, an indication is provided to upper layers. In addition to an indication to respond to the AIoT paging message or the AIoT identification information, the lower layers provide the $RAND_{AIOT\_n}$ value included in the AIoT paging message to AIoT NAS layer.

5.2.3 Inventory procedure completion

The AIoT device determines to respond to the AIoT paging:

a) based on the indication from lower layer as specified in 3GPP TS 38.391 [8]; or

b) based on whether the AIoT identification information (see 3GPP TS 23.003 [5]) received from the lower layer is matched or not.

The AIoT identification information consists of two parts (see clause 31.7 of 3GPP TS 23.003 [5]):

a) AIoT identification information type; and

b) component of AIoT identification information.

The AIoT device determines whether the AIoT identification information is matched or not as follows:

a) when the AIoT identification information type is set to "indicate component of AIoT identification information is AIoT device permanent identifier" (see clause 31.2 of 3GPP TS 23.003 [5]):

   1) if privacy protection is not used and the AIoT device permanent identifier of the received AIoT identification information is the same as the AIoT device permanent identifier of the AIoT device, the AIoT device determines the AIoT identification information is matched; or

   2) otherwise, the AIoT device determines the AIoT identification information is not matched;

b) when the AIoT identification information type is set to "indicate component of AIoT identification information is AIoT device temporary identifier" (see clause 31.6 of 3GPP TS 23.003 [5]):

   1) if the T-ID type of the received AIoT device temporary identifier information is set to "concealed T-ID type", privacy protection is used and the T-ID value of the received AIoT device temporary identifier information is the same as the T-ID generated based on the AIoT device permanent identifier, the AIoT device determines the AIoT identification information is matched;

   2) if the T-ID type of the received AIoT device temporary identifier information is set to "stored T-ID type", privacy protection is used and the T-ID value of the received AIoT device temporary identifier information is the same as the locally stored T-ID of the AIoT device, the AIoT device determines the AIoT identification information is matched; or

   3) otherwise, the AIoT device determines the AIoT identification information is not matched;

c) when the AIoT identification information type is set to "indicate component of AIoT identification information is filtering information" (see clause 31.3 of 3GPP TS 23.003 [5]):

   1) if all the filtering elements in the filtering information are matched, the AIoT device determines the AIoT identification information is matched. A filtering element is considered as matched if:

      A) the filtering type of the filtering element is set to "indicate the filtering type for the filtering element is ID Type", and the component value of the filtering element is the same as the corresponding bitstring from the ID type of the AIoT device permanent identifier based on the offset field and the length field;

      B) the filtering type of the filtering element is set to "indicate the filtering type for the filtering element is PLMN ID" and:

         i) the PLMN ID field is included in the AIoT device permanent identifier; and

         ii) the PLMN ID field in the AIoT device permanent identifier is the same as the component value of the filtering element;

      C) the filtering type of the filtering element is set to "indicate the filtering type for the filtering element is NID" and:

         i) the NID field is included in the AIoT device permanent identifier; and

         ii) the NID field in the AIoT device permanent identifier is the same as the component value of the filtering element;

D) the filtering type of the filtering element is set to "indicate the filtering type for the filtering element is third party identifier" and:

i) the third party identifier field is included in the AIoT device permanent identifier; and

ii) the third party identifier field in the AIoT device permanent identifier is the same as the component value of the filtering element; or

E) the filtering type of the filtering element is set to "indicate the filtering type for the filtering element is identification information", and the component value of the filtering element is the same as the corresponding bitstring from the identification information of the AIoT device permanent identifier based on the offset field and the length field; or

2) otherwise, the AIoT device determines the AIoT identification information is not matched.

NOTE 1: It is allowed to limit only the leftmost n bits of the AIoT device permanent identifier to be used for matching purpose by local configuration (see clause 5.4.2 of 3GPP TS 33.369 [6]). In this case, any filtering element that requires to match the not allowed bit(s) is considered as not matched.

NOTE 2: The AIoT identification information corresponds to the paging ID, as defined in 3GPP TS 38.391 [8].

Based on whether the AIoT identification information is matched:

a) if the AIoT identification information is matched, the AIoT device shall indicate to the lower layer that the AIoT identification information is matched, and determine to respond to the AIoT paging; or

b) otherwise, the AIoT device shall ignore the AIoT identification information, indicate to the lower layer that the AIoT identification information is not matched, and determine not to respond to the AIoT paging.

If the AIoT device determines to respond to the AIoT paging, the AIoT device shall send an INVENTORY REPORT message to the AIOTF.

The AIoT device shall derive a $RAND_{AIOT\_d}$ value as specified in 3GPP TS 33.369 [6] and shall include the derived $RAND_{AIOT\_d}$ value in the $RAND_{AIOT\_d}$ IE in the INVENTORY REPORT message.

The AIoT device shall derive a RES_{AIOT} value, using the long-term K_{AIoT_root}, the generated $RAND_{AIOT\_d}$ and the value of the $RAND_{AIOT\_n}$ included in the paging message provided by lower layers as specified in 3GPP TS 33.369 [6]. The derived RES_{AIOT} value shall be included in the RES_{AIOT} IE in the INVENTORY REPORT message.

If privacy protection is not used, the AIoT device shall include the AIoT device permanent identifier in the AIoT device identity IE in the INVENTORY REPORT message.

If privacy protection is used, the AIoT device shall not include the AIoT device identity IE in the INVENTORY REPORT message.

If the AIoT identification information type is set to "indicate component of AIoT identification information is AIoT device temporary identifier information", the AIoT device determines the AIoT identification information is matched and the stored T-ID update indication indicates "update without command procedure", the AIoT device shall replace the locally stored T-ID with a new T-ID value calculated as specified in 3GPP TS 33.369 [6], clause B.1.

Upon all the selected NG-RAN indicating the inventory procedure has been completed, the inventory procedure is considered as completed by the AIOTF as specified in 3GPP TS 23.369 [2].

NOTE 3: How NG-RAN indicates the inventory procedure has been completed is defined in 3GPP TS 38.300 [7] and 3GPP TS 38.413 [10].

5.2.4 Inventory procedure not accepted by AIoT device

If the AIoT device has completed a permanent disable command procedure, the AIoT device shall not respond to the AIoT paging message.

5.2.5 Abnormal cases in the AIoT device

The following abnormal cases can be identified:

a) AIoT paging collision of AIoT paging.

   If a new AIoT paging is received while an inventory procedure is in progress, the AIoT device shall abort the ongoing inventory procedure and shall proceed with the new AIoT paging.

5.2.6 Abnormal cases in the AIOTF

The following abnormal cases can be identified:

a) Lower layer failure

   In the case the lower layer indication of an inventory failure received as specified by 3GPP TS 38.413 [10] from all the selected NG-RAN(s), the AIOTF shall abort the inventory procedure.

   In the case the lower layer indication of no inventory response from all the selected NG-RAN(s), the AIOTF shall abort the inventory procedure.

5.3 Command procedures

5.3.1 General

This clause describes command procedures between the AIOTF and AIoT device. Command procedures are initiated by the AIOTF to perform read, write, or permanent disable operation on the AIoT device.

5.3.2 Read command procedure

5.3.2.1 General

The purpose of the read command procedure is to retrieve AIoT data from the AIoT device (see example in figure 5.3.2.1.1).

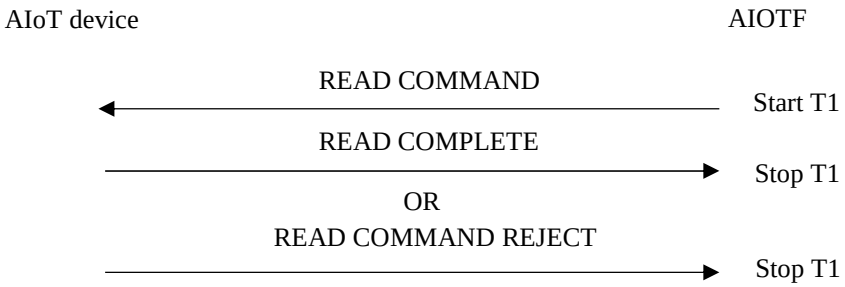

Figure 5.3.2.1.1: Read command procedure

5.3.2.2 Read command procedure initiation

The AIOTF initiates the read command procedure by sending a READ COMMAND message to the AIoT device and starting the timer T1. In the READ COMMAND message, the AIOTF:

a) shall include the Read offset IE set to the offset from the start of the AIoT device's user memory, indicating where to read the AIoT data;

b) shall include the Read length IE set to the length of the AIoT data to be read; and

c) shall include the AIoT device T-ID IE set to the new AIoT device T-ID when the stored T-ID update indication is set to "update with command procedure" in the preceding AIoT paging message.

5.3.2.3 Read command procedure accepted by the AIoT device

Upon receiving the READ COMMAND message, if the AIoT device supports read command, the AIoT device:

a) shall validate the offset in the Read offset IE and the length in the Read length IE;

NOTE: The validation of the offset and the length is implementation-specific to the AIoT device.

b) shall retrieve the AIoT data based on the Read offset IE and the Read length IE which are validated in a);

c) if the AIoT device T-ID IE is received in the READ COMMAND message and the SPI field in the Security header IE is set to "Integrity protected and ciphered with 128-NEA2", shall replace the previously stored AIoT device T-ID, if any, with the received AIoT device T-ID; and

d) shall send a READ COMPLETE message to the AIOTF.

In the READ COMPLETE message, the AIoT device shall include the AIoT data IE set to the retrieved AIoT data described in b).

Upon receiving of the READ COMPLETE message, if the new AIoT device T-ID was included in the READ COMMAND message, the AIOTF shall consider the new AIoT device T-ID as valid and the old AIoT device T-ID, if any, as invalid.

5.3.2.4 Read command procedure completion by the AIOTF

Upon receiving the READ COMPLETE message, the AIOTF shall consider the read command procedure as successfully completed and stop the timer T1.

5.3.2.5 Read command procedure not accepted by AIoT device

Upon receiving a READ COMMAND message, if the command type specific parameter (e.g. the offset to read application data from the AIoT Device user memory, the length of the application data to read.) is invalid, the AIoT device shall send a READ COMMAND REJECT message with a cause set to #1 "Command type specific parameters invalid".

Upon receiving a READ COMMAND message, if the read command procedure cannot be performed because the energy will run out, the AIoT device shall send a READ COMMAND REJECT message with a cause set to #3 "Low energy".

Upon receiving the READ COMMAND REJECT message, the AIOTF shall consider the read command procedure is unsuccessful and stop timer T1.

5.3.2.6 Abnormal cases in the AIoT device

The following abnormal cases can be identified:

a) The read command is unsuccessfully executed (e.g. user memory operation error).

The AIoT device shall send a READ COMMAND REJECT message with a cause set to #111 "Error, unspecified".

b) AIoT paging collision.

If a new AIoT paging is received while a read command procedure is in progress, the AIoT device shall abort the ongoing read command procedure and shall proceed with the new AIoT paging.

NOTE: In this release of the specification, implementation-specific mechanisms can be applied to avoid the collision case.

5.3.2.7 Abnormal cases in the AIOTF

The following abnormal cases can be identified:

a) Lower layer failure

In the case the lower layer indication of a command failure received as specified by 3GPP TS 38.413 [10], the AIOTF shall abort the read command procedure and the AIOTF shall consider both the old T-ID and the new T-ID as valid until one of these T-IDs can be considered as invalid. The AIOTF may initiate a T-ID sequence recovery as specified in clause 5.4.4 of 3GPP TS 33.369 [6] to resolve the T-ID conflict.

b) Expiry of timer T1

The AIOTF shall abort the read command procedure, consider the read command procedure is unsuccessful and the AIOTF shall consider both the old T-ID and the new T-ID as valid until one of these T-IDs can be considered as invalid. The AIOTF may initiate a T-ID sequence recovery as specified in clause 5.4.4 of 3GPP TS 33.369 [6] to resolve the T-ID conflict.

5.3.3 Write command procedure

5.3.3.1 General

The purpose of the write command procedure is to write the AIoT data to the AIoT device's user memory (see example in figure 5.3.3.1.1).

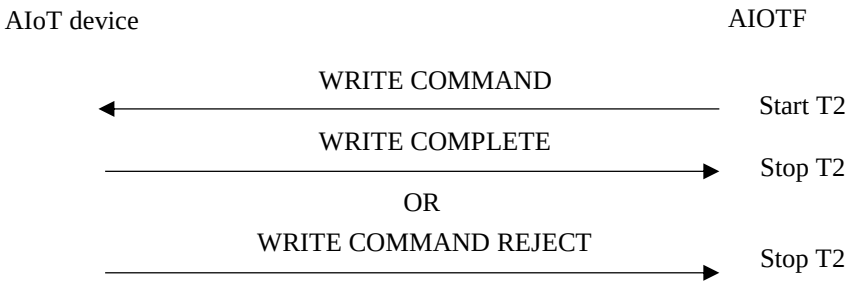

Figure 5.3.3.1.1: Write command procedure

5.3.3.2 Write command procedure initiation

The AIOTF initiates the write command procedure by sending a WRITE COMMAND message to the AIoT device and starting the timer T2. In the WRITE COMMAND message, the AIOTF:

a) shall include the Write offset IE set to the offset from the start of the AIoT device's user memory indicating where to write the AIoT data;

b) shall include the AIoT data IE set to the AIoT data to be written; and

c) shall include the AIoT device T-ID IE set to the new AIoT device T-ID when the stored T-ID update indication is set to "update with command procedure" in the preceding AIoT paging message.

5.3.3.3 Write command procedure accepted by AIoT device

Upon receiving the WRITE COMMAND message, if the AIoT device supports write command, the AIoT device:

a) shall validate the offset in the Write offset IE and the length of AIoT data contents in the AIoT data IE;

NOTE: The validation of the offset and the length is implementation-specific to the AIoT device.

b) shall write the AIoT data contents in the received AIoT data IE to the AIoT device's user memory at the offset which is validated in a);

c) if the AIoT device T-ID IE is received in the WRITE COMMAND message and the SPI field in the Security header IE is set to "Integrity protected and ciphered with 128-NEA2", shall replace the previously stored AIoT device T-ID, if any, with the received T-ID; and

d) shall send a WRITE COMPLETE message to the AIOTF.

Upon receiving of the WRITE COMPLETE message, if the new AIoT device T-ID was included in the WRITE COMMAND message, the AIOTF shall consider the new AIoT device T-ID as valid and the old AIoT device T-ID, if any, as invalid.

5.3.3.4 Write command procedure completion by the AIOTF

Upon receiving the WRITE COMPLETE message, the AIOTF shall consider the write command procedure as successfully completed and stop the timer T2.

5.3.3.5 Write command procedure not accepted by AIoT device

Upon receiving a WRITE COMMAND message, if the command type specific parameter (e.g. the offset where to write the application data, the length of the application data to write) is invalid, the AIoT device shall send a WRITE COMMAND REJECT message with a cause set to #1 "Command type specific parameters invalid".

Upon receiving a WRITE COMMAND message, if the write command procedure cannot be performed because the energy will run out, the AIoT device shall send a WRITE COMMAND REJECT message with a cause set to #3 "Low energy".

Upon receiving the WRITE COMMAND REJECT message, the AIOTF shall consider the write command procedure is unsuccessful and stop timer T2.

5.3.3.6 Abnormal cases in the AIoT device

The following abnormal cases can be identified:

a) The write command is unsuccessfully executed (e.g. user memory operation error)

   The AIoT device shall send a WRITE COMMAND REJECT message with a cause set to #111 "Error, unspecified".

b) AIoT paging collision.

   If a new AIoT paging is received while a write command procedure is in progress, the AIoT device shall abort the ongoing write command procedure and shall proceed with the new AIoT paging.

NOTE: In this release of the specification, implementation-specific mechanisms can be applied to avoid the collision case.

5.3.3.7 Abnormal cases in the AIOTF

The following abnormal cases can be identified:

a) Lower layer failure

   In the case the lower layer indication of a command failure received as specified by 3GPP TS 38.413 [10], the AIOTF shall abort the write command procedure and the AIOTF shall consider both the old T-ID and the new T-ID as valid until one of these T-IDs can be considered as invalid. The AIOTF may initiate a T-ID sequence recovery as specified in clause 5.4.4 of 3GPP TS 33.369 [6] to resolve the T-ID conflict.

b) Expiry of timer T2

   The AIOTF shall abort the write command procedure, consider the write command procedure is unsuccessful and the AIOTF shall consider both the old T-ID and the new T-ID as valid until one of these T-IDs can be considered as invalid. The AIOTF may initiate a T-ID sequence recovery as specified in clause 5.4.4 of 3GPP TS 33.369 [6] to resolve the T-ID conflict.

5.3.4 Permanent disable command procedure

5.3.4.1 General

The purpose of the permanent disable command procedure (see example in figure 5.3.4.1.1) is to permanently disable the communication capability of the AIoT device as specified in 3GPP TS 23.369 [2].

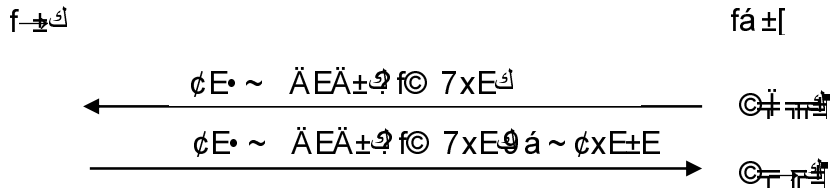

Figure 5.3.4.1.1: Permanent disable command procedure

5.3.4.2 Permanent disable command procedure initiation

The AIOTF initiates the permanent disable command procedure by sending a PERMANENT DISABLE COMMAND message to the AIoT device and starting the timer T3.

5.3.4.3 Permanent disable command procedure accepted by AIoT device

Upon receiving the PERMANENT DISABLE COMMAND message, the AIoT device shall send a PERMANENT DISABLE COMPLETE message to the AIOTF and disable the communication capability of the AIoT device.

5.3.4.4 Permanent disable command procedure completion by the AIOTF

Upon receiving the PERMANENT DISABLE COMPLETE message, the AIOTF shall consider the permanent disable command procedure as successfully completed and stop the timer T3.

5.3.4.5 Abnormal cases in the AIoT device

The following abnormal cases can be identified:

a) AIoT paging collision.

   If a new AIoT paging is received while a permanent disable command procedure is in progress, the AIoT device shall abort the ongoing permanent disable command procedure and shall proceed with the new AIoT paging.

NOTE: In this release of the specification, implementation-specific mechanisms can be applied to avoid the collision case.

5.3.4.6 Abnormal cases in the AIOTF

The following abnormal cases can be identified:

a) Lower layer failure

   In the case the lower layer indication of a command failure received as specified by 3GPP TS 38.413 [10], the AIOTF shall abort the permanent disable command procedure.

b) Expiry of timer T3

   The AIOTF shall abort the permanent disable command procedure and consider the permanent disable command procedure is unsuccessful.

NOTE: In the case that the network determines to permanently disable an AIoT device as specified in clause 5.2.2.3 in 3GPP TS 23.369 [2] and the permanent disable command procedure was unsuccessful due to expiry of the timer T3, the network can take this into account for further actions for the AIoT device.

5.4 Common procedures

5.4.1 Status procedure

5.4.1.1 General

The purpose of the sending of the STATUS message is to report certain error conditions detected in a received AIoT NAS message by the AIoT device (see example in figure 5.4.1.1.1). The STATUS message shall be integrity protected. The same ciphering shall apply to the STATUS message as the ciphering in the received AIoT NAS message that triggers the STATUS message.

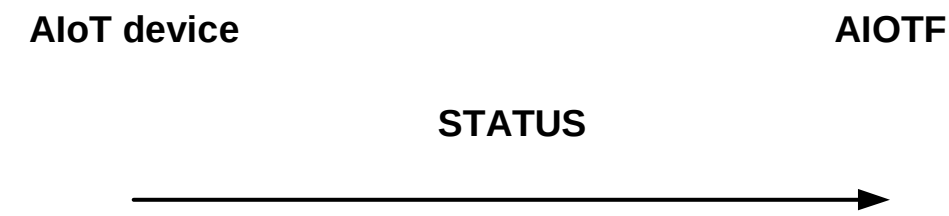

Figure 5.4.1.1.1: Status procedure

5.4.1.2 Status procedure initiation

The AIoT device initiates the status procedure by sending a STATUS message to the AIOTF as described in clause 6.

5.4.1.3 Status procedure completion by the AIOTF

If the AIOTF receives a STATUS message the AIOTF shall take different actions depending on the received cause value:

#97 message type non-existent or not implemented.

The AIOTF shall abort any ongoing AIoT NAS procedure related to the AIoT device and stop any related timer.

NOTE: If the read command procedure or the write command procedure was aborted due to reception of the STATUS message with the cause #97 "message type non-existent or not implemented", the network can take this into account to avoid initiating further command procedures of the same command type towards the AIoT device, in order to save unnecessary signalling wasting radio resources.

The local actions to be taken by the AIOTF on receipt of a STATUS message with any other cause values are implementation dependent.

6 Handling of unknown, unforeseen, and erroneous protocol data

6.1 General

The procedures specified in the present document apply to those messages which pass the checks described in this clause.

This clause also specifies procedures for the handling of unknown, unforeseen, and erroneous protocol data by the receiving entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the protocols.

Clauses 6.2 to 6.7 shall be applied in order of precedence.

Detailed error handling procedures in the network are implementation dependent and may vary from network to network. However, when extensions of this protocol are developed, networks will be assumed to have the error handling that is indicated in this clause as mandatory ("shall") and that is indicated as strongly recommended ("should").

Also, the error handling of the network is only considered as mandatory or strongly recommended when certain thresholds for errors are not reached during a dedicated connection.

For definition of semantical and syntactical errors see 3GPP TS 24.007 [3], clause 11.4.2.

In this release of the specification, conditional IEs and comprehension required IEs are not supported by the AIoT NAS protocol.

6.2 Message too short or too long

6.2.1 Message too short

When a message is received that is too short to contain a complete message type information element, that message shall be ignored, c.f. 3GPP TS 24.007 [3], and the AIoT device shall provide an indication to the lower layers that the message was ignored.

6.2.2 Message too long

The AIoT device and the AIOTF shall not send an AIoT NAS message larger than the maximum size to prevent exceeding the value range for upper layer data specified in 3GPP TS 38.391 [8].

NOTE: In this release of the specification, the maximum size of an AIoT NAS message allowed to be sent by the AIoT device is 125 octets, while the maximum size of an AIoT NAS message allowed to be sent by the AIOTF is 119 octets.

6.2A Unknown or unforeseen security protection indication

If the network receives an AIoT NAS message with a Security header IE including a security protection indication parameter value not defined for the AIoT NAS protocol or not implemented by the receiver, it shall ignore the AIoT NAS message.

If the AIoT device receives an AIoT NAS message with a Security header IE including a security protection indication value not defined for the AIoT NAS protocol or not implemented by the receiver, the AIoT device shall ignore the message and provide an indication to the lower layers that the message was ignored.

6.3 Unknown or unforeseen message type

If the network receives an AIoT NAS message with a message type not defined for the AIoT NAS protocol or not implemented by the receiver, it shall ignore the AIoT NAS message.

If the AIoT device receives an AIoT NAS message with a message type not defined for the AIoT NAS protocol or not implemented by the receiver, it shall return a STATUS message with cause #97 "message type non-existent or not implemented".

NOTE: A message type not defined for the AIoT NAS protocol in the given direction is regarded by the receiver as a message type not defined for the AIoT NAS protocol, see 3GPP TS 24.007 [3].

6.4 Non-semantical mandatory information element errors

6.4.1 Common procedures

When on receipt of a message,

a) an "imperative message part" error; or

b) a "missing mandatory IE" error;

is diagnosed or when a message containing a syntactically incorrect mandatory IE is received,

a) the AIoT device shall:

- if the message is not one of the messages listed in clause 6.4.2, the AIoT device shall ignore the message and return a STATUS message with cause #96 "invalid mandatory information"; and

b) the network shall either:

- try to treat the message (the exact further actions are implementation dependent); or

- ignore the message.

6.4.2 Specific AIoT procedures

The following procedures shall apply when the AIoT device encounters an error with a mandatory information element in an AIoT NAS message:

a) If the message is a READ COMMAND, then a READ COMMAND REJECT message with cause #96 "invalid mandatory information", shall be returned; and

b) if the message is a WRITE COMMAND, then a WRITE COMMAND REJECT message with cause #96 "invalid mandatory information", shall be returned.

6.5 Unknown and unforeseen IEs in the non-imperative message part

6.5.1 IEIs unknown in the message

The AIoT device shall ignore all IEs with unknown IEI in a message.

The network shall take the same approach.

6.5.2 Out of sequence IEs

The AIoT device shall ignore all out of sequence IEs in a message.

The network should take the same approach.

6.5.3 Repeated IEs

If an information element with format T, TV or TLV is repeated in a message, the AIoT device shall handle only the contents of the information element appearing first and shall ignore all subsequent repetitions of the information element.

The network should follow the same procedures.

6.6 Non-imperative message part errors

6.6.1 General

This category includes syntactically incorrect optional IEs.

6.6.2 Syntactically incorrect optional IEs

The AIoT device shall treat all optional IEs that are syntactically incorrect in a message as not present in the message.

The network shall take the same approach.

6.7 Messages with semantically incorrect contents

When a message with semantically incorrect contents is received, the AIoT device shall perform the foreseen reactions of the procedural part of clause 5. If, however no such reactions are specified, the AIoT device shall ignore the message and provide an indication to the lower layers.

When a message with semantically incorrect contents is received, the AIOTF shall perform the foreseen reactions of the procedural part of clause 5. If, however no such reactions are specified, the AIOTF shall ignore the message.

7 Encoding of AIoT NAS protocol

7.1 Message functional definitions and contents

7.1.1 General

Within the AIoT NAS protocol defined in the present document, every message is a standard L3 message as defined in 3GPP TS 24.007 [3]. This means that the message consists of the following parts:

1) if the message is an unprotected AIoT NAS message:
   a) security header;
   b) message type; and
   c) other information elements, as required.
2) if the message is a security protected AIoT NAS message:
   a) security header;
   b) message authentication code;
   c) message type; and
   d) other information elements, as required.

The organization of an unprotected AIoT NAS message is illustrated in the example shown in figure 7.1.1-1.

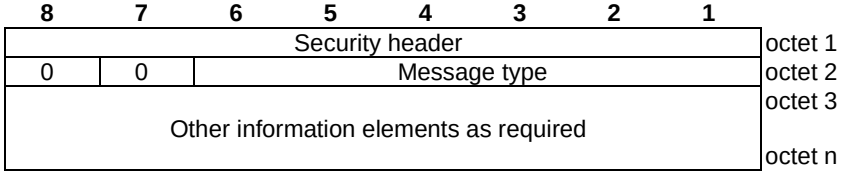

Figure 7.1.1-1: General message organization example for an unprotected AIoT NAS message

The INVENTORY REPORT message is an unprotected AIoT NAS message.

The organization of a security protected AIoT NAS message is illustrated in the example shown in figure 7.1.1-2.

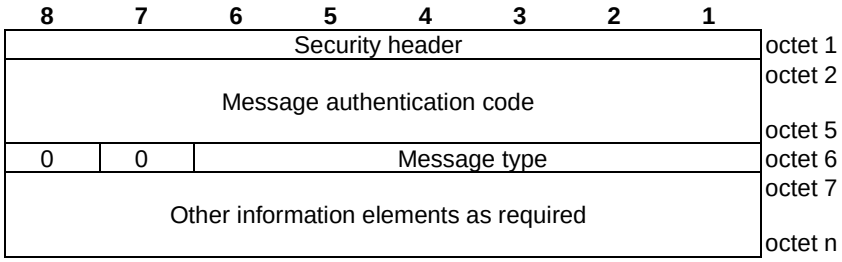

Figure 7.1.1-2: General message organization example for a security protected AIoT NAS message

All AIoT NAS messages except the INVENTORY REPORT message are security protected AIoT NAS messages.

7.1.2 Inventory report

7.1.2.1 Message definition

The INVENTORY REPORT message is sent by the AIoT device to the AIOTF to reply to the AIoT paging.

See table 7.1.2.1-1.

Message type: INVENTORY REPORT

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.2.1-1: INVENTORY REPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message type	Message type 7.2.2	M	V	1
	$RAND_{AIOT\_d}$	RAND 7.2.12	M	V	16
	RES_{AIOT}	Authentication response parameter 7.2.8	M	V	8
11	AIoT device identity	AIoT device identity 7.2.6	O	TLV	7-77

7.1.2.2 AIoT device identity

This IE shall be included when the AIoT device needs to provide its AIoT device permanent identifier to the AIOTF.

7.1.3 Read command

7.1.3.1 Message definition

The READ COMMAND message is sent by the AIOTF to the AIoT device to read the AIoT data from the memory.

See table 7.1.3.1-1.

Message type: READ COMMAND

Significance: dual

Direction: AIOTF to AIoT device

Table 7.1.3.1-1: READ COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Read command message identity	Message type 7.2.2	M	V	1
	Read offset	Offset 7.2.11	M	V	2
	Read length	AIoT data length 7.2.5	M	V	1
10	AIoT device T-ID	AIoT device T-ID 7.2.7	O	TV	17

7.1.3.2 AIoT device T-ID

This IE shall be included in the message when the AIOTF needs to provide a new T-ID to the AIoT device as specified in clause 5.3.2.2.

7.1.4 Read complete

7.1.4.1 Message definition

The READ COMPLETE message is sent by the AIoT device to the AIOTF to provide the AIoT data that has been read from the memory.

See table 7.1.4.1-1.

Message type: READ COMPLETE

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.4.1-1: READ COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Read complete message identity	Message type 7.2.2	M	V	1
	AIoT data	AIoT data 7.2.4	M	LV	2-85

7.1.5 Read command reject

7.1.5.1 Message definition

The READ COMMAND REJECT message is sent by the AIoT device to the AIOTF to indicate the cause of the failure of reading the AIoT data from the memory.

See table 7.1.5.1-1.

Message type: READ COMMAND REJECT

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.5.1-1: READ COMMAND REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Read command reject message identity	Message type 7.2.2	M	V	1
	Read cause	Cause 7.2.9	M	V	1

7.1.6 Write command

7.1.6.1 Message definition

The WRITE COMMAND message is sent by the AIOTF to the AIoT device to write the indicated AIoT data to the memory.

See table 7.1.6.1-1.

Message type: WRITE COMMAND

Significance: dual

Direction: AIOTF to AIoT device

Table 7.1.6.1-1: WRITE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Write command message identity	Message type 7.2.2	M	V	1
	Write offset	Offset 7.2.11	M	V	2
	AIoT data	AIoT data 7.2.4	M	LV	2-85
10	AIoT device T-ID	AIoT device T-ID 7.2.7	O	TV	17

7.1.6.2 AIoT device T-ID

This IE shall be included in the message when the AIOTF needs to provide a new T-ID to the AIoT device as specified in clause 5.3.3.2.

7.1.7 Write complete

7.1.7.1 Message definition

The WRITE COMPLETE message is sent by the AIoT device to the AIOTF to indicate that the AIoT data has been successfully written to the memory.

See table 7.1.7.1-1.

Message type: WRITE COMPLETE

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.7.1-1: WRITE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Write complete message identity	Message type 7.2.2	M	V	1

7.1.8 Write command reject

7.1.8.1 Message definition

The WRITE COMMAND REJECT message is sent by the AIoT device to the AIOTF to indicate the cause of the failure of writing the AIoT data from the memory.

See table 7.1.8.1-1.

Message type: WRITE COMMAND REJECT

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.8.1-1: WRITE COMMAND REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Write command reject message identity	Message type 7.2.2	M	V	1
	Write cause	Cause 7.2.9	M	V	1

7.1.9 Permanent disable command

7.1.9.1 Message definition

The PERMANENT DISABLE COMMAND message is sent by the AIOTF to the AIoT device to permanently disable the communication capability of AIoT device.

See table 7.1.9.1-1.

Message type: PERMANENT DISABLE COMMAND

Significance: dual

Direction: AIOTF to AIoT device

Table 7.1.9.1-1: PERMANENT DISABLE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Permanent disable command message identity	Message type 7.2.2	M	V	1

7.1.10 Permanent disable complete

7.1.10.1 Message definition

The PERMANENT DISABLE COMPLETE message is sent by the AIoT device to the AIOTF to indicate that the AIoT device communication capability has been disabled.

See table 7.1.10.1-1.

Message type: PERMANENT DISABLE COMPLETE

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.10.1-1: PERMANENT DISABLE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Permanent disable complete message identity	Message type 7.2.2	M	V	1

7.1.11 STATUS

7.1.11.1 Message definition

The STATUS message is sent by the AIoT device to the AIOTF to report certain error conditions listed in clause 6.

See table 7.1.11.1-1.

Message type: STATUS

Significance: dual

Direction: AIoT device to AIOTF

Table 7.1.11.1-1: STATUS message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Security header	Security header 7.2.3	M	V	1
	Message authentication code	Message authentication code 7.2.10	M	V	4
	Status message identity	Message type 7.2.2	M	V	1
	Status cause	Cause 7.2.9	M	V	1

7.2 Encoding of information elements

7.2.1 General

This clause describes the encoding of the information elements used in the messages of the AIoT NAS protocol.

7.2.2 Message type

The Message type IE and its use are defined in 3GPP TS 24.007 [3]. Table 7.2.2.1 defines the value part of the Message type IE used in the AIoT NAS protocol.

Table 7.2.2-1: Message types for AIoT NAS

Bits						
6	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	1	Inventory report
0	0	0	0	1	0	Read command
0	0	0	0	1	1	Read complete
0	0	0	1	0	0	Read command reject
0	0	0	1	0	1	Write command
0	0	0	1	1	0	Write complete
0	0	0	1	1	1	Write command reject
0	0	1	0	0	0	Permanent disable command
0	0	1	0	0	1	Permanent disable complete
0	0	1	0	1	0	Status
Bits 8 and 7 are encoded as "0"; other values are reserved for possible future protocol extensions. A protocol entity expecting an AIoT NAS message with bits 8 and 7 encoded as "0" and receiving a message containing bit 8 or bit 7 encoded as "1" shall diagnose an "unknown or unforeseen message type" error and treat the message as specified in clause 6.3.						

7.2.3 Security header

The purpose of the security header information element is to indicate security related properties for the message in which the information element is included as first octet.

The security header information element is coded as shown in figure 7.2.3-1 and table 7.2.3-1.

The security header information element is a type 3 information element with length of 2 octets.

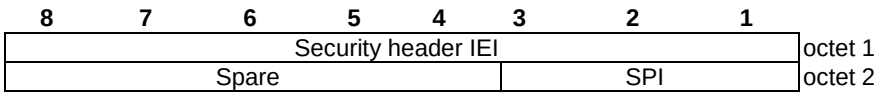

Figure 7.2.3-1: Security header information element

Table 7.2.3-1: Security header information element

Security protection indication (SPI) (octet 2, bit 1 to 3)			
Bits			
3	**2**	**1**	
0	0	0	Unprotected AIoT NAS message
			Security protected AIoT NAS message:
0	0	1	Integrity protected with 128-NIA2 and ciphered with NEA0
0	1	0	Integrity protected with 128-NIA2 and ciphered with 128-NEA2
Bits 4 to 8 of octet 2 are spare and shall be coded as zero.			

7.2.4 AIoT data

The purpose of the AIoT data information element is to carry the AIoT data that has been read from the memory or that is to be written to the memory of the AIoT device.

The AIoT data information element is coded as shown in figure 7.2.4-1 and table 7.2.4-1.

The AIoT data is a type 4 information element with a minimum length of 3 octets and a maximum length of 86 octets.

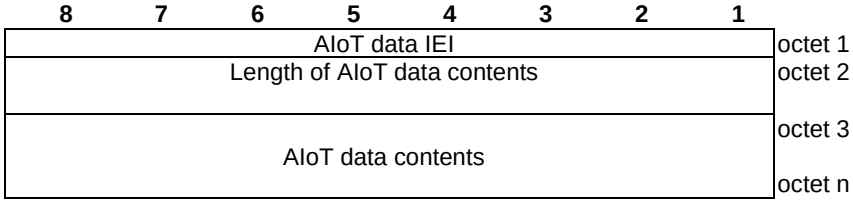

Figure 7.2.4-1: AIoT data information element

Table 7.2.4-1: AIoT data information element

AIoT data contents (octets 3 to n): The AIoT data contents contain the contents of the AIoT data that has been read from the memory or that is to be written in the memory of the AIoT device. The maximum length of the AIoT data contents field is 84 octets.

7.2.5 AIoT data length

The purpose of the AIoT data length information element is to indicate the length of the AIoT data to be read in a read operation.

The AIoT data length information element is coded as shown in figure 7.2.5-1 and table 7.2.5-1.

The AIoT data length is a type 3 information element with length of 2 octets.

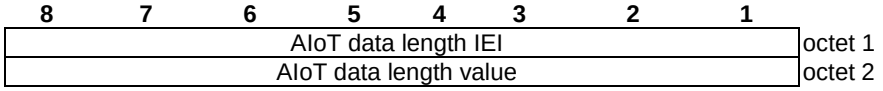

Figure 7.2.5-1: AIoT data length information element

Table 7.2.5-1: AIoT data length information element

AIoT data length value (octet 2) This field contains the length of data to be read from AIoT device memory.

7.2.6 AIoT device identity

The purpose of the AIoT device identity information element is to provide the network with the AIoT device identity of the AIoT device.

The AIoT device identity information element is coded as shown in figure 7.2.6-1 and table 7.2.6-1.

The AIoT device identity is a type 4 information element with minimum length of 7 octets and maximum length of 77 octets.

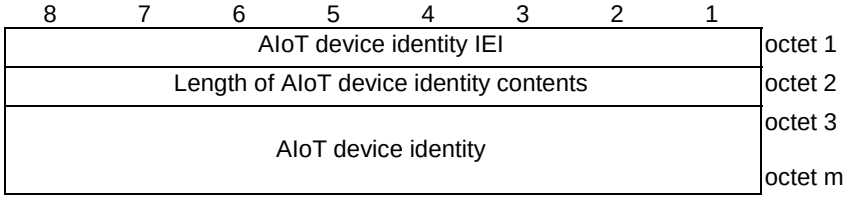

Figure 7.2.6-1: AIoT device identity information element

Table 7.2.6-1: AIoT device identity

AIoT device identity(octets 3 to m) This field is encoded as the structure of AIoT device permanent identifier as specified in clause 31.2 in 3GPP TS 23.003 [5]. When the ID Type is set to "NID part is included", bits 5 to 8 of the last octet of the NID field are coded as zero.

7.2.7 AIoT device T-ID

The purpose of the AIoT device T-ID information element is to provide the AIoT device T-ID to the AIoT device.

The AIoT device T-ID information element is coded as shown in figure 7.2.7-1 and table 7.2.7-1.

The AIoT device T-ID is a type 3 information element with length of 17 octets.

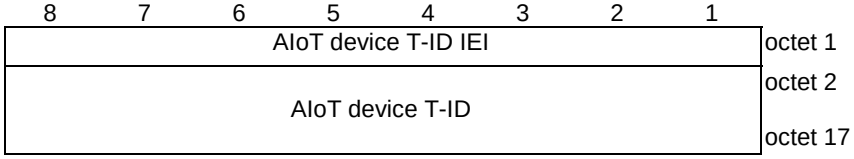

Figure 7.2.7-1: AIoT device T-ID information element

Table 7.2.7-1: AIoT device T-ID

AIoT device T-ID (octets 2 to 17) This field is encoded as the structure of AIoT device temporary identifier as specified in 3GPP TS 23.003 [5].

7.2.8 Authentication response parameter

The purpose of the authentication response parameter information element is to provide the network with the authentication response calculated in the AIoT device.

The Authentication response parameter information element is coded as shown in figure 7.2.8-1 and table 7.2.8-1.

The Authentication response parameter is a type 3 information element with 9 octets length. In an AIoT authentication challenge, the response calculated in the AIoT device is 8 octets in length, and is placed in the Authentication response parameter information element.

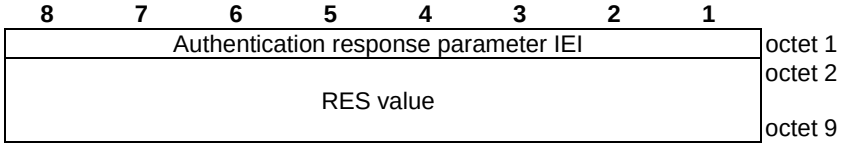

Figure 7.2.8-1 Authentication response parameter information element

Table 7.2.8-1: Authentication response parameter information element

RES value (octet 2 to 9) The RES value consists of 64 bits. Bit 8 of octet 2 is the most significant bit while bit 1 of octet 9 is the least significant bit.

7.2.9 Cause

The purpose of the cause information element is to indicate the cause of the failure of the AIoT NAS message.

The cause information element is coded as shown in figure 7.2.9-1 and table 7.2.9-1.

The cause is a type 3 information element with length of 2 octets.

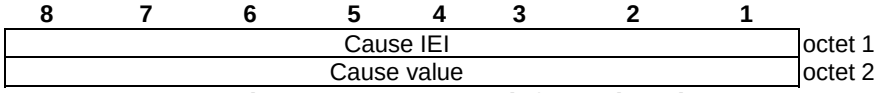

Figure 7.2.9-1: Cause information element

Table 7.2.9-1: Cause information element

Cause value (octet 2)	
Bits **8 7 6 5 4 3 2 1**	
0 0 0 0 0 0 0 1	Command type specific parameters invalid
0 0 0 0 0 0 1 1	Low energy
0 1 1 0 0 0 0 0	Invalid mandatory information
0 1 1 0 0 0 0 1	Message type non-existent or not implemented
0 1 1 0 1 1 1 1	Error, unspecified
All other values are spare and if received shall be interpreted as 0110 1111, "Error, unspecified".	

7.2.10 Message authentication code

The purpose of the Message authentication code information element is to protect the integrity of an AIoT NAS message.

The Message authentication code is a type 3 information element with 5 octets length.

The Message authentication code information element is coded as shown in figure 7.2.10-1 and table 7.2.10-1.

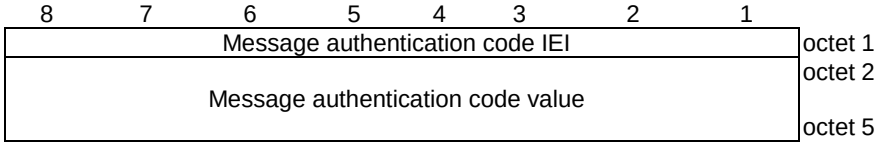

Figure 7.2.10-1: Message authentication code information element

Table 7.2.10-1: Message authentication code information element

Message authentication code value (octet 2 to 5) This field contains the 32 bit message authentication code calculated for AIoT integrity protection. Bit 8 of octet 2 is the most significant bit, and bit 1 of octet 5 is the least significant bit of these 4 octets.

7.2.11 Offset

The purpose of the Offset information element is to provide the AIoT device offset indication, i.e. where to read the AIoT data from or where to write the AIoT data to.

The Offset information element is coded as shown in figure 7.2.11-1 and table 7.2.11-1.

The Offset is a type 3 information element with a length of 3 octets.

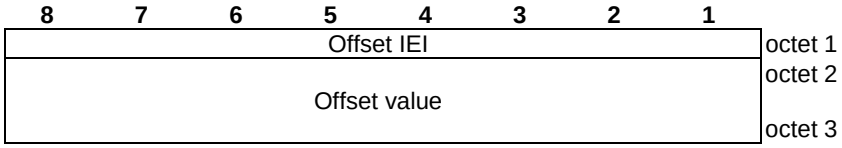

Figure 7.2.11-1 Offset information element

Table 7.2.11-1: Offset information element

Offset value (octet 2 to 3) This field contains 2 octet offset value. Bit 8 of octet 2 is the most significant bit, and bit 1 of octet 3 is the least significant bit.

7.2.12 RAND

The purpose of the RAND information element is to provide the AIoT device or the AIOTF with a non-predictable number to be used in security calculations.

The RAND information element is coded as shown in figure 7.2.12-1 and table 7.2.12-1.

The RAND is a type 3 information element with 17 octets length.

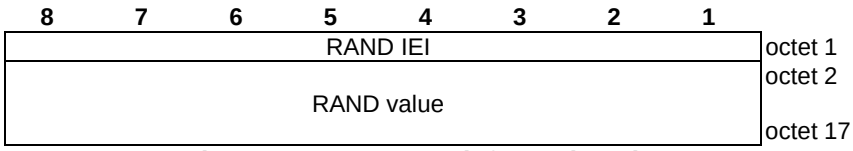

Figure 7.2.12-1 RAND information element

Table 7.2.12-1: RAND information element

RAND value (octet 2 to 17) The RAND value consists of 128 bits. Bit 8 of octet 2 is the most significant bit while bit 1 of octet 17 is the least significant bit.

8 List of system parameters

8.1 General

This clause describes the definition of the timers for AIoT.

8.2 Timers of command procedure

Timers of command procedure are shown in table 8.2-1.

Table 8.2-1: Timers of command procedure – AIOTF side

TIMER NUM.	TIMER VALUE	DEFINITION	CONDITION OF START	NORMAL STOP	ON EXPIRY
T1	NOTE	Timer for the read command procedure	Read command procedure initiated	Read command procedure completed or rejected. STATUS message received.	Abort the read command procedure and consider the read command procedure is unsuccessful.
T2	NOTE	Timer for the write command procedure	Write command procedure initiated	Write command procedure completed or rejected. STATUS message received.	Abort the write command procedure and consider the write command procedure is unsuccessful.
T3	NOTE	Timer for the permanent disable command procedure	Permanent disable command procedure initiated	Permanent disable command procedure completed.	Abort the permanent disable command procedure and consider the permanent disable command procedure is unsuccessful.
NOTE: The value of this timer is network dependent.					

Annex A (informative): Cause values

A.1 Cause values for the AIoT NAS protocol

Cause #1 – Command type specific parameters invalid

This cause is used to indicate that the command type specific parameter (e.g. the offset to read application data from the AIoT device user memory, the length of the application data to read, the offset where to write the application data, or the length of the application data to write) is invalid.

Cause #3 – Low energy

This cause is used to indicate that the command procedure cannot be performed because the energy will run out.

Cause #96 – Invalid mandatory information

This cause is used to indicate that the equipment sending this cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This cause is used to indicate that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this cause.

Cause #111 – Error, unspecified

This cause is used to indicate that the requested read or write command was not executed successfully.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2025-04	CT1#154					TS skeleton draft. C1-252552, C1-252553.	0.1.0
2025-05	CT1#155					Inclusion of pCRs agreed during CT1#155: C1-253642, C1-253643, C1-253754, C1-253756, C1-254097, C1-254111, C1-254112, C1-254133.	0.2.0
2025-08	CT1#156					Inclusion of pCRs agreed during CT1#156: C1-255166, C1-255170, C1-255186, C1-255189, C1-255286, C1-255330, C1-255623, C1-255624, C1-255625, C1-255626, C1-255643, C1-255644, C1-255646, C1-255647, C1-255660, C1-255661, C1-255675, C1-255704.	0.3.0
2025-09	CT#109	CP-252116				Presenting 3GPP TS 24.369 to CT#109 for information.	1.0.0
2025-10	CT1#157					Inclusion of pCRs agreed during CT1#157: C1-256042, C1-256289, C1-256291, C1-256310, C1-256467, C1-256531, C1-256534, C1-256537, C1-256538, C1-256540, C1-256630, C1-256631, C1-256635, C1-256636, C1-256637, C1-256640, C1-256643, C1-256647, C1-256664, C1-256667, C1-256881, C1-256887, C1-256895.	1.1.0
2025-11	CT1#158					Inclusion of pCRs agreed during CT1#158: C1-257013, C1-257299, C1-257410, C1-257414, C1-257415, C1-257495, C1-257500, C1-257501, C1-257504, C1-257508, C1-257509, C1-257511, C1-257512, C1-257517, C1-257521, C1-257522, C1-257523, C1-257525, C1-257563, C1-257566, C1-257568, C1-257597, C1-257598, C1-257599, C1-257600, C1-257617, C1-257632, C1-257633, C1-257634, C1-257638	1.2.0
2025-12	CT#110	CP-253069				Presenting 3GPP TS 24.369 to CT#110 for approval.	2.0.0
2025-12	CT#110	CP-253069				Approved by TSG CT.	19.0.0
2026-03	CT#111	CP-260121	0005	1	F	Clarification on handling of AIoT identification information	19.1.0
2026-03	CT#111	CP-260121	0006	1	F	Clarification on the indication from lower layers when handling of paging request	19.1.0
2026-03	CT#111	CP-260121	0010		F	Parameter alignment	19.1.0
2026-03	CT#111	CP-260121	0011	1	F	Missing optional IE clauses	19.1.0
2026-03	CT#111	CP-260121	0013	2	F	AIoT data IE maximum size	19.1.0
2026-03	CT#111	CP-260121	0014	1	F	T-ID length	19.1.0
2026-03	CT#111	CP-260121	0016	2	F	RES length	19.1.0
2026-03	CT#111	CP-260121	0018	3	F	Undefined security header codepoints	19.1.0
2026-03	CT#111	CP-260121	0019	1	F	Indicate the integrity failure to the lower layer	19.1.0
2026-03	CT#111	CP-260121	0022	2	F	Cause#3 in Read Command Reject	19.1.0
2026-03	CT#111	CP-260121	0024	2	F	Handling of T-ID due to lower layer failue	19.1.0
2026-03	CT#111	CP-260121	0025	1	F	Miscellaneous corrections	19.1.0
2026-03	CT#111	CP-260121	0026	1	F	Alignment of "AIoT paging message" terminology	19.1.0
2026-03	CT#111	CP-260121	0027		F	Clarification on AIoT NAS message in ciphering	19.1.0
2026-03	CT#111	CP-260121	0029	1	F	Correction to the length of AIoT device identity IE	19.1.0
2026-03	CT#111	CP-260122	0032		F	AIoT Authentication correction	19.1.0
2026-03	CT#111	CP-260122	0033	1	F	Correction to stored T-ID update indication	19.1.0
2026-03	CT#111	CP-260122	0034	1	F	Correction to T-ID inclusion in command message	19.1.0
2026-03	CT#111	CP-260122	0037		F	Correction on usage of privacy protection	19.1.0
2026-03	CT#111	CP-260122	0039	1	F	Correction on redundant description, optional device id, and the paging name	19.1.0

History

Version	Date	Status
V19.0.0	February 2026	Publication
V19.1.0	March 2026	Publication