ETSI TS 133 369 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

5G;
Security aspects of Ambient Internet of Things (AIoT) services for isolated private networks
(3GPP TS 33.369 version 19.0.0 Release 19)

Reference

DTS/TSGS-0333369vj00

Keywords

5G,SECURITY

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

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 security and privacy aspects of AIoT services in the 5G System (5GS), complying to the requirements in TS 22.369 [4], applicable to the AIoT Device types, traffic types, use cases and connectivity topologies defined in TS 38.300 [3], and based on the architecture defined in TS 23.369 [2].

The AIoT system is defined as private network, i.e. isolated network deployment that does not interact with a public network, e.g. an SNPN.

Security features for AIoT services include:

1. Network Layer Authentication between AIoT device and 5G core

   a. AIOTF is the endpoint in the 5G core

   b. Credentials are securely stored in the ADM on the network side

   NOTE 1: The credentials are assumed to be stored in a secure environment in the ADM. How this is realized is left to implementation. The requirements will reflect this.

   c. Secure storage and processing of credentials in the AIoT device.

   NOTE 2: For SNPN deployment the storage of the credentials of non-AKA based methods is out of scope as described in TS 33.501[5] Annex I 2.2.

   d. Security aspects of the storage of the credentials at the ADM

2. Confidentiality, anti-replay and integrity protection of information during AIoT service communication

3. Privacy of AIoT device identifiers using the AIoT Temp ID.

4. Security to protect the permanent disabling RF transmission capabilities of AIoT device(s).

Editor's Note: Further refinement is FFS.

2 References

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

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

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

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

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

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

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

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

[7] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA"

3 Definitions of terms, symbols 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 Device: as specified in TS 23.369 [2].

3.2 Symbols

Void

3.3 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 Internet of Things
AIOTF	Ambient IoT Function

4 Security requirements for AIoT service

4.1 General

Two functional cases are supported: inventory, command.

The AIoT RAN reader is assumed to be trusted, i.e., authorized from network side to communicate with the AIoT device.

4.2 Security Requirements

4.2.1 Requirements on the device

4.2.1.1 Secure storage and processing of credentials

The long-term credentials used for authentication shall be securely stored and processed on the AIoT device.

The long-term credentials shall be protected against cloning when stored or processed.

The long-term credentials shall be confidentiality and integrity protected when stored and processed.

In the present document, the AIoT system is defined as private network (isolated network deployment that does not interact with a public network) e.g. SNPN, and the AIoT device credentials storage follows 3GPP defined requirements, the exact mechanism is out of scope of 3GPP (similar to Annex I.2.2 of TS 33.501 [5]). This means that no interconnection exists between AIoT systems and PLMNs.

NOTE 1: In case UICC is used, the exact form factor and whether it is removable, non-removable or integrated is out of scope of 3GPP.

NOTE 2: UICC provides protection for long-term credentials against physical and logical attacks.

4.2.1.2 Requirements related to authentication between device and network

The AIoT device shall support:

- a method for pseudo-random bit generation.

Editor’s Note: Further cryptographic primitives are FFS.

4.2.1.3 Requirements for command protection

The AIoT device shall support confidentiality protection of AIoT NAS messages between the AIoT device and the AIOTF.

Confidentiality protection of AIoT NAS messages between the AIoT device and the AIOTF is optional to use.

The AIoT device shall support the following ciphering algorithms:

NEA0 and 128-NEA2 as specified in Annex D of TS 33.501 [5].

The AIoT device shall support integrity protection and replay protection of AIoT NAS messages between the AIoT device and the AIOTF.

Integrity protection of AIoT NAS messages between the AIoT device and the AIOTF is mandatory to use.

The AIoT device shall support the following integrity algorithms:

128-NIA2 as specified in Annex D of TS 33.501 [5].

4.2.1.4 Requirements for identifier privacy

- The device shall support a mechanism for the use of temporary IDs.

Editor's Note: this requirement will be revisited.

4.2.2 Requirements on the AIOTF

4.2.2.1 Requirement on Authentication

The AIOTF shall authenticate the AIoT device.

4.2.2.2 Requirements on Communication Protection

The AIOTF shall support confidentiality protection of AIoT NAS Command request and response between the AIoT device and the AIOTF.

The AIOTF shall support the following ciphering algorithms:

NEA0, 128-NEA2 as defined in Annex D of the TS 33.501 [5].

Confidentiality protection of AIoT NAS Command request and response between the AIoT device and the AIOTF is optional to use.

The AIOTF shall support integrity protection of AIoT NAS Command request and response between the AIoT device and the AIOTF.

The AIOTF shall support the following integrity algorithms:

128-NIA2 as defined in Annex D of the TS 33.501 [5].

Integrity protection of AIoT NAS Command request and response between the AIoT device and the AIOTF is mandatory to use.

The AIOTF shall support selection of confidentiality and integrity algorithms for protecting AIoT NAS Command request and response between the AIoT device and the AIOTF based on operator's local policy.

4.2.2.3 Requirements on Privacy

The AIOTF shall support a mechanism for the use of temporary IDs and it is optional for network to use.

4.2.3 Requirements on the ADM

For network layer authentication between AIoT device and 5G core, credentials shall be securely stored in the ADM. In case of SNPN, AIoT device credential can be stored in the credential holder instead of ADM.

NOTE: Security mechanisms for storage of AIoT device credentials in the ADM are left to implementation.

4.2.4 Security Requirements on the NG-RAN

AIOT2 is the reference point between the AIOTF and the NG-RAN.

NG-RAN shall support the use of integrity, confidentiality and replay protection with the AIOTF over the AIOT2 interface.

5 Security procedures for Ambient IoT service

5.1 General

This clause describes the security procedures for Ambient IoT service. The requirements can be found in clause 4.

5.2 Authentication procedure

5.2.1 General

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

Editor's Note: The alignment with the ID privacy procedure is FFS.

NOTE: K_{AIOT_root} is the long-term key.

5.2.2 Authentication procedure

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

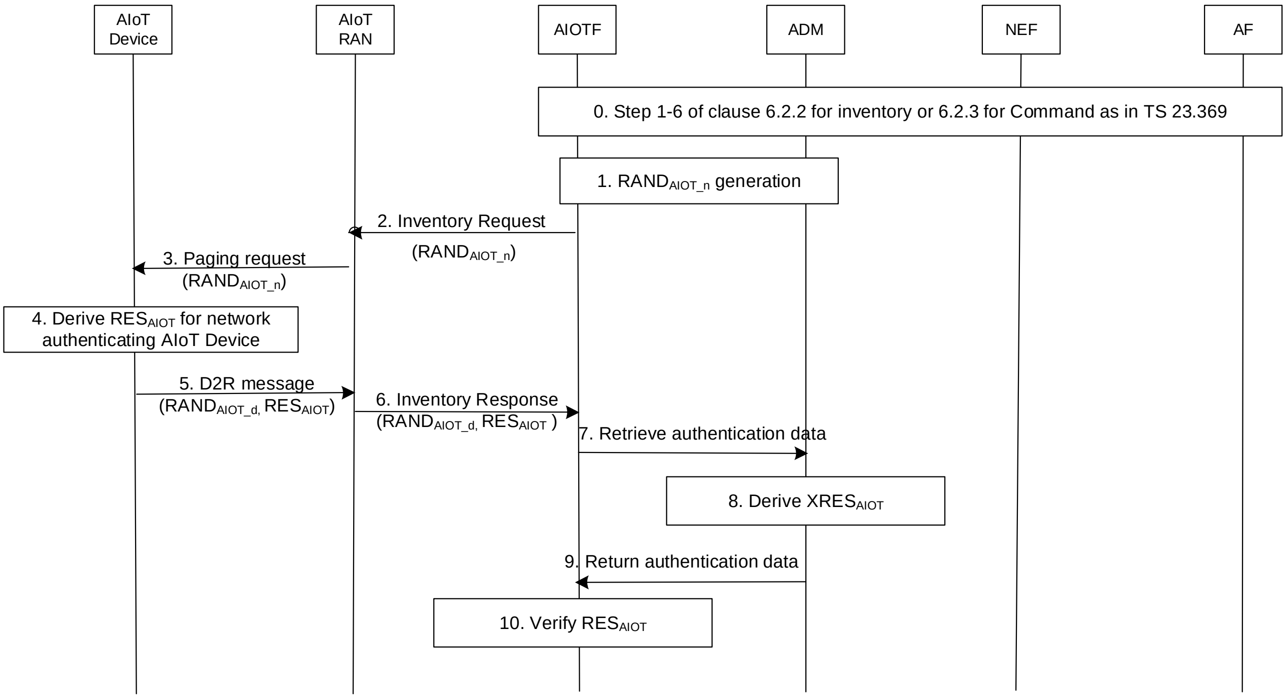
AIoT Device
AIoT RAN
AIOTF
ADM
NEF
AF
0. Step 1-6 of clause 6.2.2 for inventory or 6.2.3 for Command as in TS 23.369
1. $RAND_{AIOT\_n}$ generation
2. Inventory Request ($RAND_{AIOT\_n}$)
3. Paging request ($RAND_{AIOT\_n}$)
4. Derive RES_{AIOT} for network authenticating AIoT Device
5. D2R message ($RAND_{AIOT\_d}$, RES_{AIOT})
6. Inventory Response ($RAND_{AIOT\_d}$, RES_{AIOT})
7. Retrieve authentication data
8. Derive $XRES_{AIOT}$
9. Return authentication data
10. Verify RES_{AIOT}

Figure 5.2.1-1: Authentication procedure

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

1. ADM shall generate $RAND_{AIOT\_n}$. AIOTF shall retrieve $RAND_{AIOT\_n}$ from ADM.

2. AIOTF shall send inventory request message including $RAND_{AIOT\_n}$ to NG-RAN.

3. NG-RAN shall include $RAND_{AIOT\_n}$ in the paging request message to the AIoT device in addition to other device identification information.

NOTE 1: An active attack may send a new paging request to the device while there is an ongoing procedure in device. The device will abort the ongoing procedure and respond to the new paging. The security measure to such denial-of-service attack is not specified in present document.

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

4. Upon receiving the paging request message, if the device determines it needs to respond based on the device identification information, AIoT device shall generate $\text{RAND}_{\text{AIOT\_d}}$, calculate RES_{AIOT} using $\text{K}_{\text{AIoT\_root}}$ and $\text{RAND}_{\text{AIOT\_n}}$ (see Annex A.2) for network authenticating AIoT Device.

Editor's Note: the randomness of $\text{RAND}_{\text{AIOT\_d}}$ is FFS.

5. AIoT device sends D2R message to the NG-RAN, including RES_{AIOT} and $\text{RAND}_{\text{AIOT\_d}}$ from device.

6. NG-RAN sends Inventory report message to AIOTF, including the RES_{AIOT} and $\text{RAND}_{\text{AIOT\_d}}$.

7. AIOTF sends device identification information, $\text{RAND}_{\text{AIOT\_n}}$ and $\text{RAND}_{\text{AIOT\_d}}$ to ADM.

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

8. ADM shall calculate $\text{XRES}_{\text{AIOT}}$ using the same method as in AIoT device (see Annex A.2).

9. ADM sends $\text{XRES}_{\text{AIOT}}$ to AIOTF.

10. AIOTF verifies RES_{AIOT}. If the verification is successful, for command case, AIOTF shall acquire K_{AIoTF} from ADM. ADM shall calculate K_{AIoTF} if receiving request from AIOTF (see AnnexA.2). ADM sends K_{AIoTF} to AIOTF.

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

For the command procedure, the AIoT device implicitly authenticates the network via the verification of MAC which is derived using the $\text{K}_{\text{Command\_int}}$ as specified in clause 5.3.2 of present document.

5.3 Protection of information during AIoT service communication

5.3.1 General

This clause describes the security procedures for the information protection in command message. The protection of information is provided as part of the AIoT NAS protocol between AIoT device and AIOTF. The AIOTF acts as the security termination point for AIoT information protection.

5.3.2 Security procedure on information protection during command procedure

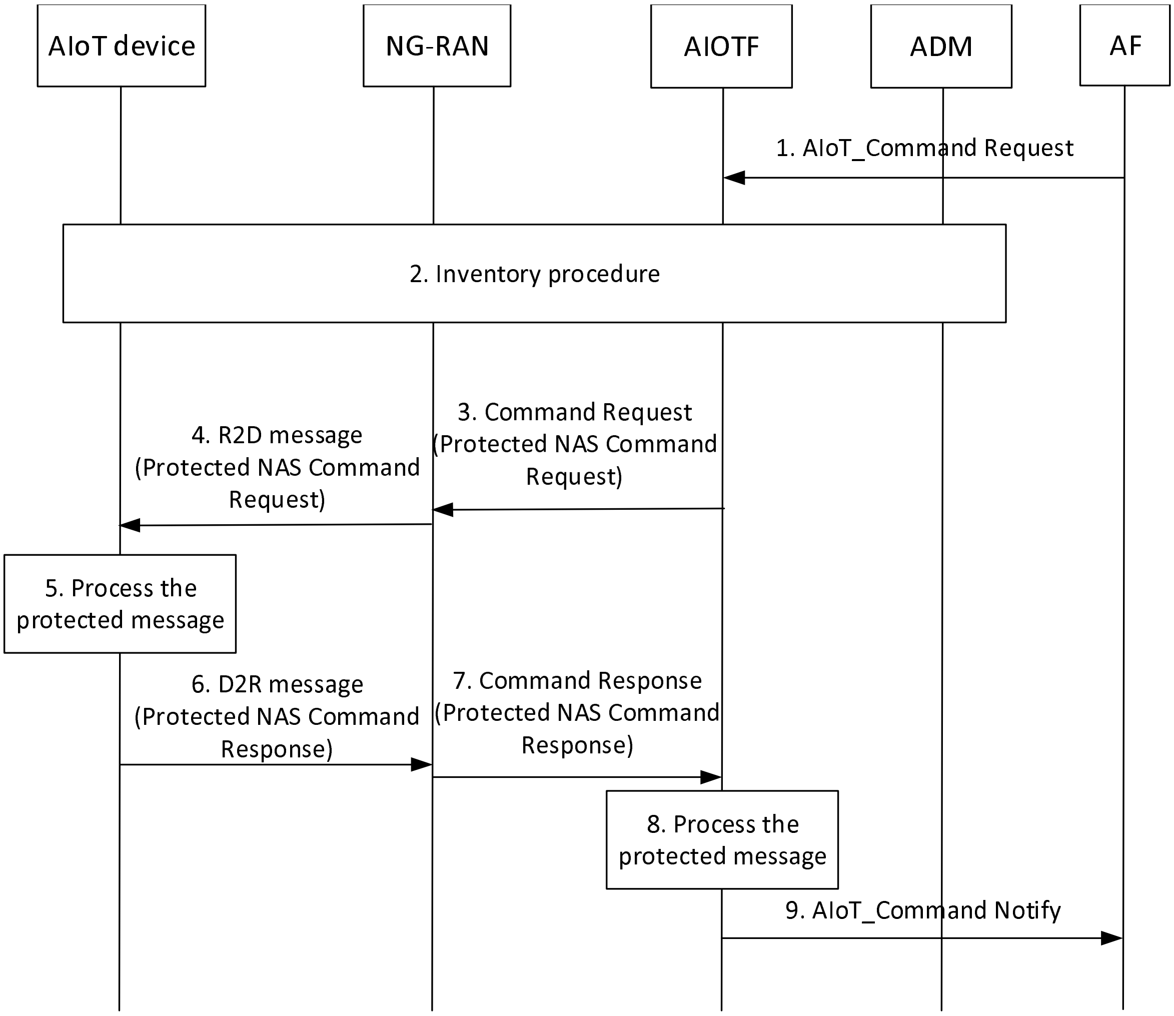
AIoT device
NG-RAN
AIOTF
ADM
AF
1. AIoT_Command Request
2. Inventory procedure
3. Command Request (Protected NAS Command Request)
4. R2D message (Protected NAS Command Request)
5. Process the protected message
6. D2R message (Protected NAS Command Response)
7. Command Response (Protected NAS Command Response)
8. Process the protected message
9. AIoT_Command Notify

Figure 5.3.2-1: Security procedure on the information protection during command procedure

1. The command procedure is initiated as specified in step 1-6 of clause 6.2.3 of TS 23.369 [2].

2. The procedure as described in clause 5.2.2 shall be performed. The device and AIOTF acquire the K_{AIOTF} key to be used for command protection. The derivation of K_{AIOTF} key is specified in Annex A.3.

3. The AIOTF shall construct a AIOT NAS Command Request and protect the message based on the $K_{Command\_enc}$, $K_{Command\_int}$, the confidentiality and integrity algorithms for the AIoT device. The AIOTF shall send the protected Command Request containing an indication on whether cyphering is activated to NG-RAN.

NOTE 1: The whole AIOT NAS Command Request message is integrity protected. If confidentiality algorithm is not null-scheme, the AIOT NAS Command Request message is partly ciphered with the exception that the selected protection algorithms are in clear text.

4. The NG-RAN shall send a R2D message containing the protected AIOT NAS Command Request as specified in as specified in TS 38.300 [3] and TS 38.391 [6].

5. The device shall derive the $K_{Command\_enc}$, $K_{Command\_int}$ and verify the integrity of the command message. If the verification of integrity is successful, the AIoT device shall decipher it in case it is confidentiality protected. The AIoT device shall construct a NAS Command Response and protect the message based on the $K_{Command\_enc}$ and $K_{Command\_int}$ key using the same algorithms.

6. The AIoT device shall send a D2R message containing the protected AIOT NAS Command Response to the NG-RAN as specified in as specified in TS 38.300 [3] and TS 38.391 [6].

7. The NG-RAN shall forward the AIOT NAS Command Response containing the protected AIOT NAS Command Response to the AIOTF.

8-9. The AIOTF shall verify the integrity of the command message. If the verification of integrity is successful, the AIoT device shall decipher it in case it is confidentiality protected. Then, the AIOTF shall continue the procedure as specified in clause 6.2.3 of TS 23.369 [2].

NOTE 2: It is assumed that there is only one round of command procedure per device following an inventory procedure. Since the K_{AIOTF} key is fresh, there is no need for additional freshness parameters for replay protection.

NOTE 3: It is assumed that no new algorithms will ever be introduced for information protection during command procedure.

5.3.3 Input parameters to integrity algorithm

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

The KEY input is equal to the $K_{Command\_int}$ key.

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

The BEARER is set to all zeros.

The COUNT is set to all zeros.

5.3.4 Input parameters to ciphering algorithm

The input parameters for the ciphering algorithms shall be the same as the ones used for NAS integrity protection as described in clause 5.3.3, with the exception that there is an additional input parameter, namely the length of the key stream to be generated by the ciphering algorithms and the KEY input is equal to the $K_{Command\_enc}$ key.

5.4 Protection of AIoT device identifier privacy

5.4.1 General

This clause describes the mechanisms to protect AIoT device identifier privacy during the inventory procedure. The mechanism is based on the use of a Temporary ID (i.e., T-ID). The T-ID is generated based on the key (i.e., K_{AIoT_root}) shared between AIoT device and ADM. Depending on the situation and deployment scenario, the network operator can choose which paging procedure to use.

When privacy protection is not used during the inventory procedure, the AIoT device includes its AIoT device permanent identifier as a device identification information in the procedure specified in clause 5.2.2.

5.4.2 The AIoT device identifier protection for inventory with filtering information

For the protection of AIoT device permanent ID during the inventory procedure described in clause 5.2.2, the following change shall apply:

- In step 4, the AIoT device determines it needs to reply to the NG-RAN based on the received filtering information.

NOTE 1: The attacker may obtain a AIoT device ID by performing a bitwise enumeration in multiple paging messages. To mitigate the attack, the AIoT device need to be configured with filtering information to match by limiting which bits of AIoT device identifier is allowed for filtering information (guidance would be to limit to the leftmost n bits of the permanent device identifier, e.g., only allow filtering information for the leftmost 64 bits and not respond otherwise).

- In step 5 and 6, a device identification information is not included in the D2R message and Inventory Report message.

- In step 7, filtering information is used as a device identification information if the AIOTF received it in step 0.

NOTE 2: The AIOTF identifies the AIoT device by checking the received RES_{AIoT}. Therefore, device identification information is not needed in the D2R and Inventory Report message.

NOTE 3: When inventory with filtering information is used, after receiving the D2R message, the ADM has to exhaustively derive $XRES_{AIoT}$s with all the long-term keys (i.e., K_{AIoT_root}) of the AIoT devices in the group that was paged for every $RAND_{AIoT\_d}$ received. The AIOTF then, need to check $XRES_{AIoT}$ with the received RES_{AIoT}. Therefore, the size of the group should be chosen accordingly to reduce the energy consumption, inter NF interaction, and latency.

5.4.3 Procedure for AIoT Device identifier protection with Temp ID update during Individual inventory

For the protection of AIoT device permanent identifier during the inventory procedure with AIoT device identifier described in clause 5.2.2, the following changes shall apply:

- In step 1, AIOTF shall retrieve a T-ID in addition to the $RAND_{AIOT\_n}$ from ADM. The ADM shall, based on T-ID type, either fetch the stored T-ID in the AIoT device profile or generate the T-ID as specified in Annex B.1.
- In step 2, 3 and 4, the T-ID shall be used as a device identification information.
- In step 2 and 3 the AIOTF includes indication of type of T-ID handling. T-ID can be either concealed type or stored type. The concealed type can be based on either the stored T-ID or the permanent identifier. If needed the handling also indicates whether the stored T-ID type shall be updated with or without a command. NG-RAN includes the T-ID handling in the paging message.
- In step 4, the AIoT device, based on the T-ID handling indication in the paging message, generates the T-ID in the same way as the ADM did in step 1. The AIoT device determines it needs to reply to the NG-RAN if the generated T-ID matches with the received T-ID. In case the stored T-ID update shall be done without a command, the AIoT Device generates a new Temp_ID_n+1 as specified in Annex B.1 and stores the new Temp ID_n+1.
- In step 5 and 6, a device identification information is not included in the D2R message and Inventory Report message.
- In step 7, the AIoT device permanent identifier is used as a device identification information. AIOTF requests the ADM to derive a new T-ID as specified in Annex B.1 and to store it in the AIoT Device profile.

NOTE 1: The AIOTF identifies the AIoT device by checking the received RES_{AIoT} parameter. Therefore, the device identification information is not needed in the D2R message and Inventory Report message.

NOTE 2: In case of concealed T-ID type, every AIoT devices that receive an Inventory Request with T-ID need to perform a T-ID matching by generating a T-ID based on the K_{AIoT_root} and check if the generated T-ID is matched with the received T-ID. It is assumed that the AIoT device that receive the Inventory Request has enough energy to perform this T-ID matching in addition to the Inventory procedure specified in clause 5.2.2.

NOTE 3: In case of stored T-ID type, the stored T-IDs on the device side and network side can get out-of synch. The handling of such situation is described in clause

5.4.4 Out-of-Synch detection and Resynchronization of T-ID

In case the network does not receive an Inventory Response from a AIoT Device after an Individual Inventory Request, then it can indicate that the AIoT Device and network is out-of-synch with the TIDs. The out-of-synch can happen if e.g.:

- The Inventory Response or Command Response from the Device was lost during transmission due to radio link issues e.g. interference, range, etc. in that case the AIoT Device would generate the T-ID_n+1, but the ADM would not generate the T-ID_n+1 or know that the device has received the T-ID_n+1 as it did not get any response.

- Something went wrong during the Inventory procedure e.g. the AIoT Device managed to write to the NVM but not send the inventory response or command response or the AIoT Device sent the inventory response or command response but was not able to write to the NVM.

This means that the ADM either has a T-ID that is older or newer than the T-ID in the AIoT Device. They can never be more than one off.

T-ID sequence recovery is possible if the network performs Individual Inventory with both T-ID_n-1 or T-ID_n+1. When the AIoT device responds to the network, the network adjusts the sequence, and both are in synch again.

Alternatively, the network can use concealed T-ID type using the permanent identifier and then send a command to provide a new T-ID to the device which it stores in the device.

5.5 Protection between AIoT network elements

For the interfaces specified in clause 4.3 of TS 23.369 [2], the security procedures specified in clause 13 in TS 33.501 [5] applies to the service-based interfaces within 5G core network for Ambient IoT. The mechanism described in clause 12.3 of TS 33.501 [5] applies to the NEF-AF interface.

The security mechanism specified for N2, between 5G-AN and AMF defined in clause 9.2 of TS 33.501 [5], applies to the AIOT2 interface between AIOTF and NG-RAN.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

A.1.1 General

All key derivations (including input parameter encoding) for 5GC shall be performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220 [7].

This clause specifies how to construct the input string, S, and the input key, KEY, for each distinct use of the KDF. Note that "KEY" is denoted "Key" in TS 33.220 [7].

A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [7], FC value allocated for the present document is 0xAA-0xZZ.

A.2 RES$_{\text{AIOT}}$ and XRES$_{\text{AIOT}}$ derivation function

When deriving a RES$_{\text{AIOT}}$ and XRES$_{\text{AIOT}}$ from K$_{\text{AIOT\_root}}$, the following parameters shall be used to form the input S to the KDF:

- FC = 0xZZ,
- P0 = RAND$_{\text{AIOT\_n}}$,
- L0 = length of RAND$_{\text{AIOT\_n}}$ (i.e. 0x00 0x10),
- P1 = RAND$_{\text{AIOT\_d}}$.
- L1 = length of RAND$_{\text{AIOT\_d}}$ (i.e. 0x00 0x10),
- P2 = AIoT device permanent identifier,
- L2 = length of AIoT device permanent identifier,

The input key KEY shall be K$_{\text{AIOT\_root}}$.

A.3 K$_{\text{AIOTF}}$ derivation function

When deriving a K$_{\text{AIOTF}}$ from K$_{\text{AIOT\_root}}$, the following parameters shall be used to form the input S to the KDF:

- FC = 0xZZ,
- P0 = RAND$_{\text{AIOT\_n}}$,
- L0 = length of RAND$_{\text{AIOT\_n}}$ (i.e. 0x00 0x10),
- P1 = RAND$_{\text{AIOT\_d}}$.
- L1 = length of RAND$_{\text{AIOT\_d}}$ (i.e. 0x00 0x10),

The input key KEY shall be the K$_{\text{AIOT\_root}}$.

A.4 $K_{Command\_enc}$ and $K_{Command\_int}$ derivation function

When deriving a $K_{Command\_enc}$ or $K_{Command\_int}$ from K_{AIOTF}, the following parameters shall be used to form the input S to the KDF:

- FC = 0xZZ,
- P0 = algorithm identity as specified in TS 33.501[5].
- L0 = length of algorithm identity (i.e. 0x00 0x01)

The input key KEY shall be the K_{AIOTF}.

Annex B (normative): Temporary Identifier generation functions

B.1 T-ID generation

When generating a temporary ID (i.e., T-ID) from K_{AIOT_root}, the following parameters shall be used to form the input S to the KDF:

- FC = 0xNN,
- P0 = Temp_n,
- L0 = length of Temp_n,
- P1 = $RAND_{AIOT\_n,}$
- L1 = length of $RAND_{AIOT\_n}$

The input key KEY shall be K_{AIOT_root}. The P0 input is either the stored Temp ID_n or AIoT device Permanent ID.

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
04/2025	SA3#121					Initial version	0.0.0
04/2025	SA3#121	S3-251706				Incorporated accepted contributions: S3-251702, S3-251703, S3-251784	0.1.0
05/2025	SA3#122	S3-252287				Incorporated accepted contributions: S3-252279, S3-252280, S3-252281, S3-252410, S3-252283, S3-252282, S3-252262, S3-252308, S3-252309, S3-252412, S3-252310	0.2.0
08/2025	SA3#123	S3-252941				Incorporated accepted contributions: S3-252934, S3-252942, S3-252943, S3-252944, S3-252945, S3-252996, S3-252997, S3-252998, S3-252999, S3-253051, S3-253059	0.3.0
2025/09	SA#109	SP-251005				Presented for information and approval	1.0.0
2025/09	SA#109					Upgrade to change control version	19.0.0

History

Document history		
V19.0.0	October 2025	Publication