|  |
| --- |
| 3GPP TS 33.369 V0.1.0 (2025-04) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security aspects of Ambient IoT service(Release 19) |
|   |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview of AIOT Security aspects 8

4.1 General 8

4.2 Security Requirements 8

4.2.1 Requirements on the device 8

4.2.2 Requirements on the AIOTF 8

4.2.3 Requirements on the ADM 8

5 Security procedures for Ambient IoT service 8

5.1 General 8

5.2 Authentication procedure 8

5.3 Protection of information during AIoT service communication 8

5.4 Protection of AIoT device identifier privacy 8

5.5 Protection between AIoT network elements 8

Annex <X> (informative): Change history 9

# 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].

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”.

# 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].

**AIoT Device:** as specified in TS 23.369 [2].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 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].

ADM AIoT Data Management

AIoT Ambient Internet of Things

AIOTF Ambient IoT Function

# 4 Overview of AIOT Security aspects

## 4.1 General

Editor’s Note: This clause contains the generic security principles, assumptions.

## 4.2 Security Requirements

### 4.2.1 Requirements on the device

Editor’s Note: This clause contains the security requirement on the device, including secure storage and processing of credentials.

### 4.2.2 Requirements on the AIOTF

Editor’s Note: This clause contains the security requirement on the AIOTF.

### 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.

Editor’s Note: Security mechanisms for storage of AIoT device credentials in the UDR and for the transfer of AIoT device credentials between UDR and ADM are FFS.

Editor’s Note: Storage of credentials at a credential holder in case of SNPN has not been evaluated and further updates on the above security requirement based on the evaluation is FFS.

Editor’s Note: Further requirements are FFS.

# 5 Security procedures for Ambient IoT service

## 5.1 General

Editor’s Note: This clause contains the general security aspects.

## 5.2 Authentication procedure

Editor’s Note: This clause contains the security procedures on the authentication.

## 5.3 Protection of information during AIoT service communication

Editor’s Note: This clause contains the security procedures on the information protection in command message, including protection for disabling device operation.

## 5.4 Protection of AIoT device identifier privacy

Editor’s Note: This clause contains the security procedures for AIoT device identifier privacy.

## 5.5 Protection between AIoT network elements

Editor’s Note: This clause contains the security mechanisms for protection of the network interfaces between AIoT reader and CN and within CN.

Annex <X> (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: | 0.1.0 |