|  |  |
| --- | --- |
| 3GPP TR 33.713 V0.1.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspect of Ambient IoT Services in 5G  (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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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.  © 2024, 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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Security Architecture and Assumptions 6

5 Key issues 7

5.X Key Issue #X: <Key Issue Name> 7

5.X.1 Key issue details 7

5.X.2 Security threats 7

5.X.3 Potential security requirements 7

6 Solutions 7

6.0 Mapping of solutions to key issues 7

6.Y Solution #Y: <Solution Name> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex <X> (informative): Change history 9

# Foreword

This Technical Report 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.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The present document identifies potential threats and security requirements to enable AIoT services for various use cases. Consideration for the energy and complexity constraints of AIoT devices is taken into account in identifying and developing potential security mechanisms to support AIoT services. Specifically, the present document focuses on the following:

1. Identify security and privacy and threats introduced by AIoT services for use cases captured in TS 22.369 [2], for topologies captured in RP-234058[3], and for architecture captured in TR 23-700-13[4].

2. Identify security requirements to address the identified threats.

3. Develop potential solutions that fulfil the security requirements, taking into account AIoT device constraints agreed upon in other 3GPP working groups.

NOTE 1: Enable/disable device operation is within the scope of the present document.

# 2 References

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

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

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

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

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

[2] 3GPP TS 22.369: "Service Requirements for ambient power-enabled IoT".

[3] RP-244058, RAN New SID for Study on Solution for Ambient IoT in NR.

[4] 3GPP TR 23-700-13: "Study on Architecture Support of Ambient power-enabled Internet of Things".

# 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].

**example:** text used to clarify abstract rules by applying them literally.

## 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].

<ABBREVIATION> <Expansion>

# 4 Security Architecture and Assumptions

Editor’s Note: This clause contains security architecture and assumptions to be considered for the study (e.g., per work task/KI).

## 4.X Security Architecture

## 4.Y Security Assumptions

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Protection for disabling device operation

### 5.1.1 Key issue details

As specified in TS 22.369 [2], the enable/disable device operation is used for the operator to manage the Ambient IoT device, which can enable/disable the Ambient IoT device's capability to transmit RF signals. Based on operator policy, there are two categories of disabling device operations, i.e. permanent disabling of the capability and temporary disabling of the capability.

### 5.2.2 Threats

As a management operation, the availability of Ambient IoT devices will be impacted if the disabling device operation is not securely performed. For example, if the Ambient IoT device follows the spoofed permanent/temporary disable device operation from an attacker, the Ambient IoT devices will not respond to the network either permanently, or for a period of time, leading to the Denial of Service (DOS).

### 5.2.3 Potential security requirements

The means to securely disable the Ambient IoT device(s)’s capability to transmit RF signals shall be supported.

Editor’s Note: Whether the solutions for this key issue are the same or different from those for communication protection issue is FFS.

Editor’s Note: The conclusion regarding disabling operation procedure and the roles (e.g. application owner, network operator) in SA2 should be taken into consideration in security solution and it is FFS.

## 5.2 Key Issue #2: Authorization for 5G Ambient IoT services

### 5.2.1 Key issue details

In TR 23.700-13 [4], Key Issues #1 and #3 describe the issues on the system architecture and procedure to support 5G Ambient IoT services.

In the Topology 2 as defined in TR 38.769 [2], the UE acting as the intermediate node is responsible for transferring the information between AIoT device and 5GS. If the authorization of intermediate node is not supported, the attacker can play the role of intermediate node and arbitrarily deny.

Therefore, it is necessary to study how to authorize the UE for acting as the intermediate node.

### 5.2.2 Security threats

If the 5GC cannot verify if the UE acting as an intermediate node is authorized, the attacker UE may impersonate the intermediate node. The attacker UE may then deny the 5G Ambient IoT services.

### 5.2.3 Potential security requirements

The 5GS shall be able to support the authorization of the AIoT capable UE as an intermediate node in 5G Ambient IoT services.

## 5.3 Key issue #3: Privacy by protecting AIoT device identifiers

### 5.3.1 Key issue details

5G Ambient IoT service is a type of cellular IoT communication system where Ambient IoT devices utilize harvested energy to generate RF signals for bi-directional information transmission. Ambient IoT devices are characterized by limited functions, requiring only small and infrequent data transfers.

TS 22.369 [2] clause 5.2.6 defines the following privacy-related requirements:

“The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.”

In AIoT services, identifiers of AIoT device are used to identify the device. If the identifiers associated with a device are not privacy protected (e.g., exposed over the air), an attacker (e.g., an over-the-air attacker) can identify and track an AIoT device based on the identifiers associated with the AIoT device. Thus, this key issue is to investigate potential mechanisms to privacy protect the AIoT device identifiers.

### 5.3.2 Security Threats

An attacker can identify, monitor and track an AIoT device based on the identifiers associated with the AIoT device if the identifiers are not privacy protected.

Editor’s Note: It is FFS how the above threat affects various use cases.

Editor’s Note: Security threat and requirement for potential exposure of quantity of devices after adversary broadcasts an inventory message is FFS.

### 5.3.3 Potential security requirements

Mechanisms for mitigating privacy threats (described above) by identifying, linking, and tracking the identifiers of AIoT Device(s) shall be supported.

Editor’s Note: AIoT use cases that do not need the above privacy protection mechanisms are FFS.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Editor’s Note: Each solution should be mapped here.

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 04/2004 | SA3#115Adhoc-e | S3-241648 |  |  |  | Incorporated accepted contributions S3-241477, S3-241622, S3-241630, S3-241636 | 0.1.0 |