|  |
| --- |
| 3GPP TR 33.713 V0.3.0 (2024-08) |
| 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 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.© 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 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 6

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 9

4 Architecture and Security Assumptions 9

5 Key issues 9

5.1 Key Issue #1: Protection for disabling device operation 9

5.1.1 Key issue details 9

5.1.2 Threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Authorization for 5G Ambient IoT services 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 10

5.3 Key issue #3: Privacy by protecting AIoT device identifiers 10

5.3.1 Key issue details 10

5.3.2 Security Threats 10

5.3.3 Potential security requirements 10

5.4 Key issue #4: Protection of information during AIoT service communication 11

5.4.1 Key issue details 11

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.5 Key Issue #5: Authentication in Ambient IoT service 11

5.5.1 Key issue details 11

5.5.2 Threats 11

5.5.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 12

5.X.1 Key issue details 12

5.X.2 Security threats 12

5.X.3 Potential security requirements 12

6 Solutions 12

6.0 Mapping of solutions to key issues 12

6.1 Solution #1: Ambient IoT device disabling mechanism 12

6.1.1 Introduction 12

6.1.2 Solution details 13

6.1.3 Evaluation 14

6.2 Solution #2:PCF based Service Authorization and Provisioning to UE 14

6.2.1 Introduction 14

6.2.2 Solution details 14

6.2.3 Evaluation 15

TBD 15

6.3 Solution #3: Authorization of Intermediate UE for AIoT services 15

6.3.1 Introduction 15

6.3.2 Solution details 15

6.3.3 Evaluation 16

6.Y Solution #Y: <Solution Name> 16

6.Y.1 Introduction 16

6.Y.2 Solution details 16

6.Y.3 Evaluation 16

7 Conclusions 16

Annex <X> (informative): Change history 17

# 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".

[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].

**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 Architecture and Security Assumptions

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

The following architecture and security assumptions are applied:

* The architecture assumptions and requirements for Ambient IoT services as defined in TR 23.700-13 [4] are used as architecture assumptions in this study.
* Two functional cases are considered as baseline: (1) inventory, (2) command.

# 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.

### 5.1.2 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).

### 5.1.3 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: Security solutions for this Key Issue should be aligned with the conclusion of Ambient IoT system architecture in SA2..

## 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 5G AIoT service.

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.

## 5.4 Key issue #4: Protection of information during AIoT service communication

### 5.4.1 Key issue details

As per TS 22.369 [2], Ambient power-enabled IoT (AIoT) services aim to support various use cases, including inventory taking, sensor data collection, asset tracking, and actuator control. These services intended to operate with lower power consumption and complexity than the existing IoT technologies such as eMTC, NB-IoT, and RedCap. To fulfil these requirements, AIoT devices require a communication capability.

From a security perspective, security mechanisms to protect the information transmitted during AIoT service communication need to be supported. Failure to provide such security mechanisms will lead to various attacks such as eavesdropping, manipulation and/or unauthorized transmission of the information during AIoT service communication.

Editor’s Note: Further key issue details is FFS.

### 5.4.2 Security threats

TBD.

### 5.4.3 Potential security requirements

TBD.

## 5.5 Key Issue #5: Authentication in Ambient IoT service

### 5.5.1 Key issue details

The TR 23.700-13 [4] studies the architecture support of Ambient Internet of Things (AIoT) device, considering the service requirements for ambient power-enabled IoT device. In TR 23.700-13 [4], the validation of the AIoT device identity and authentication are explicitly mentioned.

### 5.5.2 Threats

In the air interface, an attacker may impersonate the victim device and report fake identification to the network side. If the billing is based on per AIoT device’s identity, the fake identity may lead to charging problem. Whether fake identities pose a threat in case of inventory use case, is up to the individual deployments risk profile.

Editor’s Note: additional threat is FFS.

### 5.5.3 Potential security requirements

The 5G system shall provide a means to perform mutual authentication between the AIoT device and the network.

NOTE: If solution reuses the existing authentication framework (e.g., 5G-AKA, EAP-AKA’, other EAP methods for SNPN), the existing UE security requirements in TS 33.501[5] apply. Otherwise, the core network entities, if any, that are used for authentication are dedicated for Ambient IoT service.

Editor’s Note: Secure storage and processing of credentials (on the AIoT device and network side) for solution not reusing existing authentication framework as per the note above is ffs.

Editor’s Note: Whether authentication of AIoT device is mandatory is ffs.

Editor’s Note: Whether one-way authentication needs to be defined is ffs.

Editor’s Note: Whether authentication of AIoT device can be done on application layer is 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 |
| **1** | X |  |  |
| **2** |  | X |  |
| **3** |  | X |  |
|  |  |  |  |
|  |  |  |  |

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

## 6.1 Solution #1: Ambient IoT device disabling mechanism

### 6.1.1 Introduction

According to TS 22.369, the enable/disable device operations are used by the network operator to manage the Ambient IoT device’s capability to transmit RF signals. As the disabling of RF transmission capability could, according to the operator’s policy, be temporary or permanent, it is paramount to ensure that the disabling, specifically of a permanent nature, is performed securely and in a manner that allows device recovery in case the system was compromised, and an attacker has managed to issue “disable” commands to one or multiple Ambient IoT devices.

### 6.1.2 Solution details



Figure 6.1.1 – Ambient IoT device disabling mechanism

The permanent disabling of an AIoT device is performed as a two-stage operation, where initially, the AIoT device is temporarily disabled, and then, following a cool-down period (i.e., recovery time window), the AIoT device could be disabled permanently. The two-stage permanent disabling operation is performed as follows:

In Step 0, the AIoT managing function issues a temporary disable command to the Ambient IoT device. The command includes a counter T1.

Editor’s Note: Whether the AIoT managing function is an NF or an AF is FFS.

Editor’s Note: Whether the solution aligns with SA2 system architecture and procedures is FFS.

Editor’s Note: Which threats does this solution address are FFS.

In Step 1, The AIoT device, upon receiving the temporary disable command, retrieves the counter, which will be used in subsequent processing.

In Step 2, the AIoT device sends an ACK, which may contain the counter received in Step 0.

In Step 3, The AIoT managing function issues a permanent disable command to the Ambient IoT device, in which a second counter T2 is included.

In Step 4, The AIoT device, upon receiving the permanent disable command, retrieves the second counter, then checks whether the following conditions are met:

- The AIoT device RF transmission capability is temporarily disabled.

- The AIoT device checks whether the value T2 – T1 is greater or equal to the cool-down period configured in the AIoT device.

Editor’s Note: Whether the AIoT device can maintain an internal state is FFS.

If the checks succeed, the AIoT device disables its RF transmission capability permanently.

Editor’s Note: It is FFS how the AIoT device verifies that the disable command is coming from a trusted party.

Editor’s Note: Whether the AIoT device needs to acknowledge the permanent disable is FFS.

### 6.1.3 Evaluation

Editor’s Note: How the solution addresses the security requirement of KI#1 is FFS.

TBD

## 6.2 Solution #2:PCF based Service Authorization and Provisioning to UE

### 6.2.1 Introduction

This solution addresses the KI#2 Authorization for 5G Ambient IoT services.

### 6.2.2 Solution details

This solution propose to reuse the existing mechanism for 5G Prose U2N relay as specified in TS 23.304[x] with following changes:

A UE acting as an intermediate node is registered with 5GC using the existing mechanism, with some enhancements to indicate its capability of acting as an intermediate node, and is authorized as an intermediate node (UE) during the registration procedure.

For PCF based Service Authorization and Provisioning to UE, the Registration procedures as defined in clause 4.2.2.2 of TS 23.502 [x], UE Policy Association Establishment procedure as defined in clause 4.16.11 of TS 23.502 [x] and UE Policy Association Modification procedure as defined in clause 4.16.12 of TS 23.502 [x] apply with the following additions:

- If the UE indicates AIoT Capability in the Registration Request message and if the UE is authorized to use 5G AIoT service based on subscription data, the AMF selects the PCF which supports AIoT Policy/Parameter provisioning and establishes a UE policy association with the PCF for AIoT Policy/Parameter delivery.The AMF reports the authorized AIoT Capability to the selected PCF, which may determine the AIoT Policy/Parameter based on the UE's authorized AIoT Capability.

Editor’s Note: It is FFS which 5G NF performs the authorization of the intermediate UE and this needs to align with SA2

Editor’s Note: It is FFS whether the capability is included in Registration Request

### 6.2.3 Evaluation

## TBD

## 6.3 Solution #3: Authorization of Intermediate UE for AIoT services

### 6.3.1 Introduction

The solution addresses the security requirement of KI#2: Authorization for 5G Ambient IoT services. Specifically, this solution proposes a method to authorize the UE as Intermediate UE in AF-initiated AIoT service procedure. The AMF/AIoT NF select the UE based on the information provided by AF, e.g., location information or external UE ID, and then interact with the UDM to obtain the selected UE’s subscription data and check whether it is allowed to act as Intermediate UE for AIoT secvice. Only after the UE is successfully authorized as intermediate UE, the network will then perform subsequent AIoT service procedure.

### 6.3.2 Solution details

Depicted in Figure 6.3.2-1 is the authorization procedure of Intermediate UE for AIoT Services.



**Figure** **6.3.2-1: Authorization of Intermediate UE for AIoT service**

1. The UE performs the registration procedure as specified in TS 23.502 [x] with the enhancement to indicate its AIoT Intermediate node capability, and is authorized as an intermediate UE during the registration procedure.
2. The AF sends the AIoT Service Request to the AMF/AIoT NF via the NEF, including the AIoT device ID, seivice type (e.g., Inventory, Command), location information, external UE ID (GPSI).
3. The AMF/AIoT NF selects the Intermediate UE based on the information provided by AF, e.g., location information and/or GPSI, etc.

NOTE1: The selection of Intermediate UE is up to SA2 WG decision.

1. The AMF/AIoT NF sends the UE Authorization Request to the UDM with the info of the selected UE.
2. The UDM checks whether the selected UE is allowed to act as Intermediate UE against the UE's subscription data for AIoT service.

NOTE2: The relevant subscription data could be configured offline in the UDM, or provided and updated in the UDM based on the AF-initiated AIoT service requests.

1. The UDM returns the UE Authorization Response to the AMF/AIoT NF.
2. The AMF/AIoT NF sends the AIoT Service Request to the Intermediate UE, including the AIoT device ID, service type, authorized result.
3. The inventory/Command procedure is carried out.

Editor’s Note: Whether the Intermediate UE is authorized during the registration or after the Intermediate UE selection is FFS.

Editor’s Note: Which entity performs the Intermediate UE authorization should be aligned with the AIoT system designed by SA2, which is FFS.

### 6.3.3 Evaluation

TBD

## 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** |
| 04/2024 | SA3#116Adhoc-e | S3-241476 |  |  |  | Initial draft TR | 0.0.0 |
| 04/2024 | SA3#115Adhoc-e | S3-241648 |  |  |  | Incorporated accepted contributions S3-241477, S3-241622, S3-241630, S3-241636 | 0.1.0 |
| 05/2024 | SA3#116 | S3-242536 |  |  |  | Incorporated accepted contributions S3-242649, S3-242534, S3-242535, S3-242539, S3-242540, S3-242541 | 0.2.0 |
| 08/2024 | SA3#117 | S3-243699 |  |  |  | Incorporated accepted contributions S3-243492, S3-243680 | 0.3.0 |