**3GPP TSG-SA3 Meeting #115 draft\_S3-240296-r1
Athens, Greece, February 26 – March 1, 2024**

**Source: OPPO, Apple, BUPT, Cable Labs, CATR, CATT, China Mobile, China Telecom, China Unicom, FutureWei, HiSilicon, Huawei, Intel, Inter Digital, KPN, Lenovo, Philips International B.V., Samsung, T-Mobile USA, Verizon, Vivo, Xiaomi, Xidian University, ZTE, Ericsson**

**Title: New SID on Ambient IoT Security**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

# Title: Study on Security Aspect of Ambient IoT Services in 5G

## Acronym: FS\_AIOT\_Sec

## Unique identifier: *TBA*

## Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X | X | X |  |
| No |  |  |  |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | Work Task |
| X | Study Item |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| FS\_AmbientIoT | SA1 | 950004 | R19 Study on Ambient power-enabled Internet of Things |
| FS\_Ambient\_IoT\_RAN | RAN | 970078 | R18 Study on Ambient IoT (Internet of Things) in RAN |
| AmbientIoT | SA1 | 1020030 | R19 Stage 1 of Ambient power-enabled Internet of Things |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work Items (if any) |
| Unique ID | Title | Nature of relationship |
| 1020071 | Study on Architecture support ofAmbient power-enabled Internet of Things | R19 SA2 AIoT study focuses on architectural impact and solutions to address the service and system requirements that have been identified by SA1 and RAN.  |
| 1020085 | Study on solutions for Ambient IoT (Internet of Things) in NR | R19 RAN AIoT study focuses on solutions for Ambient IoT in NR to address requirements that have been identified by RAN. |

Dependency on non-3GPP (draft) specification: N/A

# 3 Justification

5G Ambient IoT (AIoT) services are cellular IoT communication systems where 5G AIoT devices utilize harvested energy to generate RF signals for bi-directional information transmission. 5G AIoT services are characterized by support of widespread deployment of low-cost, ultra-low complexity devices with limited functions, requiring only small and infrequent data transfers and without the need for batteries.

Security aspects of CIoT and NB-Iot have been studied and specified for devices that are more capable than the expected AIoT devices. However, since AIoT devices are characterized to be limited in terms of power, computing, and storage capabilities, existing security mechanisms that are specified in the current specifications (e.g., security mechanisms supporting CIoT or NBIoT services) may prove challenging. Applying existing 5G security mechanisms to AIoT services in an inadequate manner may allow attackers to attempt to compromise the data/signalling confidentiality and integrity for different connections and interfaces.

3GPP SA1 work group has identified a set of use cases and requirements in the Rel-19 that are captured in TR 22.840 and TS 22.369, respectively. The requirements are focused on secured communication between 5GS and trusted third parties, Ambient IoT device life cycle management, flexible Ambient IoT service and configuration deployment, charging support, positioning/location detection/recognition, network capability exposure as well as security and privacy support.

RAN Rel-19 study on Ambient IoT focuses on providing clear differentiation, i.e. addressing use cases and scenarios that *cannot* otherwise be fulfilled based on existing 3GPP LPWA IoT technology e.g. NB-IoT including with reduced peak Tx power and will be captured in TR 38.769.

A complementary Rel-19 SID in SA2 has been agreed to study the stage-2 architecture solutions to address the service and system requirements that have been identified by SA1 and RAN as described above with details to be captured in TR 23.700-13.

Based on the above considerations, it is important to study the security impacts to support AIoT services in the 5G system. In particular, this SID studies whether and how existing security mechanisms (e.g., CIoT, Best, NB-IoT, etc.) specified for constrained devices in 5G can be applied to AIoT services, and if not, what security enhancements are needed.

# 4 Objective

The objectives of this study are to focus on identifying potential threats and security requirements to enable secure AIoT services for various use cases in 5G. The objectives also include analysis of what existing security mechanisms in 5G the AIoT devices can run, and what alternative security mechanism may be required. Specifically, the objectives are:

1. Identify security threats introduced by AIoT services in 5GS for each use case, e.g., inventory management, topologies, architectural and procedural enhancements, e.g., enabling/disabling AIoT devices as specified in other WGs in Rel-19.

2. Identify security requirements to address the identified threats.

3. Analyze whether the existing security mechanisms are feasible for AIoT devices. If AIoT devices cannot run an existing security mechanism in the 5G systemt

- Identify the gap(s), i.e., impact of such incapability on other existing security mechanism(s).

- Identify potential alternative security mechanisms that can fill the identified gap(s).

NOTE: Whether further Ambient IoT normative work in R19 is required will be checked in the future.

TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID  | TU Estimate (Study)  | TU Estimate (Normative)  | RAN Dependency (Yes/No/Maybe)   | Inter Work Tasks Dependency   |
| Objective #1 | 1.5 TU | N/A  | Maybe | Self-contained  |
| Objective #2 | 1 TU | N/A  | Maybe | Depends on Objective #1 |
| Objective #3 | 3.5Tus | N/A  | Maybe | Depends on Objective #1, 2 |

**Total TU estimates: 6**

**Total TU estimates for the normative phase: N/A**

**Total TU estimates for the study phase: 6 TUs**

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 33.xxx | Study on Security Aspest of Ambient IoT services in 5G  | TSG#105  | TSG#106 | TBD |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| N/A | N/A  | N/A  | N/A  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

SA2 is responsible for the system architectural aspects of Ambient IoT in 5G.

RAN working groups are responsible for RAN aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| OPPO |
| Apple |
| BUPT |
| Cable Labs |
| CATR |
| CATT |
| China Mobile |
| China Telecom |
| China Unicom |
| FutureWei |
| HiSilicon |
| Huawei |
| Intel |
| Inter Digital |
| KPN |
| Lenovo |
| Philips International B.V. |
| Samsung |
| T-Mobile, USA |
| Verizon |
| Vivo |
| Xiaomi |
| Xidian University |
| ZTE |
|  |