**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250120-r1**

Online, Electronic meeting, 13 -16 January 2025

**Source: Philips International B.V.**

**Title: Solution#1 update: Addressing ENs**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***SA3 is kindly requested to approve the following proposal.***

# 2 References

# 3 Rationale

*Regarding* Editor’s Note: How inventory/authentication is performed before the permanent disable command is FFS

*When an AIoT device is temporarily disabled, whether the network needs to re-enable, or permanently disable it, an authentication procedure needs to proceed the command operation. The AIoT MF indicates during the authentication procedure the action it intends to perform, and the device will only respond if the action concerns re-enabling, or permanent disabling the device.*

# 4 Detailed proposal

\*\*\* START OF CHANGES \*\*\*

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

### 6.1.1 Introduction

This solution addresses KI#1.

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 in 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 device is provisioned with a configuration determining how the device processes disabling operations. The configuration includes the required cool down period that needs to be met before a permanent “disable” command is allowed.

In Step 1a, the authentication procedure is performed between the AIoT device and the AIoT Management Function. Upon a successful run of the authentication procedure, the AIoT managing function issues a temporary disable command to the Ambient IoT device in step 1b. The command includes a counter T1.

NOTE 1: The AIoT Management Function (AIoT MF) depends on the entity that owns or manages the resource (i.e., AIoT device). If a device is owned or managed by the network, the disabling is triggered by the CN function AIoTF, otherwise, it is triggered by a 3rd party Management Function (e.g., AF) managing the device.

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

In Step 2, The AIoT device, upon receiving the temporary disable command, retrieves and stores the counter T1, which will be used in subsequent processing.

In Step 3, the AIoT device sends an ACK to the AIoT MF, which may contain the counter received in Step 0. Then, the AIoT device temporarily disables its RF transmission capability.

 NOTE 2: Following step 3, the AIoT device is limited to only performing a re-enable, or a permanent disable action.

In Step 4a, The AIoT MF pages the AIoT device and performs a mutual authentication procedure. Following a successful authentication and depending on whether the AIoT MF intends to re-enable the AIoT device (i.e., recovery scenario), or permanently disable the AIoT device. The AIoT MF sends in:

- Step 4b: a message containing an enable command to recover the AIoT device, or

- Step 4c: a message containing a permanent disable command, in which a second counter T2 is included.

NOTE 3: The messages in step1 and step3 carrying the temporary and permanent disable commands are protected using the same means of protection applicable to other commands (e.g., write), and so is the verification that the disable commands are coming from a legitimate party.

In Step 5, The AIoT device processes the received command. If the AIoT is requested to enable its RF transmission capability, the AIoT device recovers from the temporary disabled state and discards the stored counter T1. Otherwise, if the AIoT device is requested to perform a permanent disable command, it retrieves the second counter from the message, then checks whether the following conditions are met:

- The RF transmission capability is temporarily disabled.

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

If the checks succeed, the AIoT device temporarily enables its RF transmission capability to send an ACK message to the AIoT MF in step 6 confirming that the device is permanently disabling its RF transmission capability.

In Step 7, the AIoT device disables its RF transmission capability permanently.

\*\*\* END OF CHANGES \*\*\*