**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250121-r2**

Online, Electronic meeting, 13 -16 January 2025

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

**Title: Solution#1 evaluation update**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

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

# 2 References

# 3 Rationale

# 4 Detailed proposal

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

### 6.1.3 Evaluation

To mitigate the threat of unauthorized permanent disabling (e.g., through spoofed commands), the solution involves a controlled, two-stage operation for permanent disabling. By enforcing the cool-down period, the system adds an extra layer of control, allowing time for validation and potential recovery if an unauthorized command is detected.

In the solution proposed, the protection of disable commands (temporary and permanent) re-uses the same means of protection applicable to other commands (e.g., write command).

Ambient IoT device(s) need to maintain an internal state to support the security mechanism proposed by the solution.

Prior to re-enabling or permanently disabling a temporarily disabled Ambient IoT device, a mutual authentication procedure is performed. While temporarily disabled, the Ambient IoT device is limited to only performing a re-enable/permanent disable action.

Editor’s Note: Further evaluation is FFS.

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