**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250092-r1**

**Online, Electronic meeting, 13 -16 January 2025**

**Source: Samsung**

**Title: Resolving EN in solution #22**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.5.0**

**Work Item: FS\_Ambient\_IoT\_Sec**

**Comments**

This contribution proposes to resolve Editor's Note in solution #22.

**Proposed Changes**

\* \* \* First Change \* \* \* \*

## 6.22 Solution #22: Solution for protecting AIoT ID by using temporary ID

### 6.22.1 Introduction

This solution addresses key issue #3: Privacy by protecting AIoT device identifiers and key issue #5: Authentication in Ambient IoT service.

It is assumed that an AIoT device has power or computational resource limitation.

To avoid fake ID reporting, AIoTF checks the authenticity of the message by verifying the MAC which is generated using KAIoT and RANDAIoTF. In addition, one-way authentication (i.e., AIoTF authenticates AIoT device by checking the authenticity of AIoT Service Response) is performed.

It is assumed that AIoT device and AF are provisioned with AIoT device identifier and a key (K).

Editor’s Note: Alignment with conclusion from TR 23.700-13 [4] is FFS.

### 6.22.2 Solution details



Figure 6.22.2-1 AIoT ID protection call flow

0. AIoT ID and a key (K) are provisioned to the AIoT device and AF. AF generates KAIoT from K and RANDAF.

1. AF sends AIoT service request message to AIoTF (AIoT Function). This message may be sent via NEF. AIoT service request message includes Temp AIoT ID #1, RANDAF, and KAIoT.

NOTE: If this message is sent for the first time, the Temp AIoT ID #1 is the AIoT ID.

NOTE: The permanent AIoT ID is not sent except for the message which is sent to AIoT device for the first time. Although an attacker captures the permanent AIoT ID, the attacker without K cannot succeed an attack (e.g., paging the device, etc.) on the device nor network.

NOTE: Even if an attacker captures the message in step 2, the attacker cannot know whether the captured ID is permanent ID or not.

Editor’s Note: Possibility of potential known-plaintext attack is FFS.

2. AIoTF transfers AIoT service request message. This message includes RANDAIoTF, RANDAF, and Temp AIoT ID #1.

3. AIoT device derives KAIoT from K and RANDAF. After that, AIoT device generates MAC using Temp AIoT ID #1, RANDAIoTF, and KAIoT.

4. AIoT device responds with AIoT service response. The message includes RANDAIoT, Temp AIoT ID #1, and MAC. If the encryption on the response message is needed, AIoT device may use K for the encryption key.

5. After AIoTF finds KAIoT from Temp AIoT ID #1 received in step 4, AIoTF checks the authenticity of the message by verifying the MAC.

6. If the verification in step 5 is successful, AIoTF sends AIoT service response to AF. RANDAIoT and Temp AIoT ID #1 are included in this message.

7. AIoT device and AF generate Temp AIoT ID #2 from KAIoT, RANDAIoT, and Temp AIoT ID #1. The Temp AIoT ID #2 is used next time the AF requests a service to AIoT.

Editor’s Note: How to resolve synchronization issue on the temporary ID between AIoT device and network is FFS.

NOTE: Whether the key recovery attack can be performed depends on the algorithm to derive the temporary ID.

\* \* \* \* End of Changes \* \* \* \*