**3GPP TSG-SA3 Meeting #119e *S3-250056r1***

**emeeting, 13 - 17 January 2025**

**Source: Apple**

**Title: Update solution#28**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve the pCR to TR 33.713***

# References

1. TR 33.713 v0.5.0

# 3 Rationale

This contribution proposes update to solution#28.

There is an EN as following:

Editor’s Notes: How to address the synchronizaiton issue, e.g. when one AIoT device is connected to multi Readers, how to sync among those Readers on the HASH values of device IDs, is FFS.

When there are more than one Readers, it is assumed that all those Readers maintain the HASH table for this AIoT device. There is an index in the format of ID in the response in step2: ID1-1||Index, IDm-n indicates the n-th ID calculation using HASH for Device m, Index = n. With this indication, the second Reader is able to find the correct HASH value based on the original ID of this AIoT device. Therefore this EN can be removed.

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

# 

## 6.28 Solution #28: Privacy protection on AIoT device IDs

### 6.28.1 Introduction

This solution addresses key issue#3: “Mechanisms for mitigating privacy threats (described above) by identifying, linking, and tracking the identifiers of AIoT Device(s) shall be supported.”

### 6.28.2 Details

Preassumption: the AIoT device has one ID preconfigured by the manufacture (Application Function). Each device is configured with a root key, named K. K is unique for every AIoT device.

The device shall also maintain an Index to indicate to the network that how to map the HASH value to the HASH table. For example, when the Index is n, it indicates this is the n-th calculation of the HASH value of the device ID. The Index shall be sent uplink together with the HASH (device ID||Index).

A screenshot of a computer screen

Description automatically generated

Step 0a. the device is configured with one Device ID in the manufacturing time. Every ID is configured corresponding

to an Index. The initial Index value is 0.

Step 0b. the Application Function sends the Device IDs and Indexes to the AIoTF through NEF.

Step 0c. AIoTF sends the corresponding Device IDs to each Reader based on distribution policy from Application Function or local policy from MNOs.

Step 0d. Reader stores the Devices IDs and the corresponding Indexes under this Reader.

Step 1. Reader sends the paging message to the AIoT devices. Reader sends E(ID1), E(ID2), … in the paging message. The E() Function is HMAC, the key used is the root key K.

NOTE 1: According to RAN2 agreement in #116, the paging message may contain one ID (one Device ID or one group ID) or more (multiple IDs FFS in RAN2) IDs. The procedure may be updated based on RAN2 progress.

NOTE 2: IDm-n indicates the n-th ID calculation using HASH for Device m. ID1-0 indicates the original device ID. ID1-1 = HASH (ID1-0  ||(Index = 1)). When there are more than one Readers, it is assumed that all those Readers maintain the HASH table for this AIoT device. The index in the fomat can be used by the Readers to find the correct HASH value based on the original ID of this AIoT device.

Step 2: AIoT Device 1 verifies the IDs being paged, if verification is successful and one of the device IDs maps its ID, AIoT Device 1 confirms it was paged. Then Device 1 replies with ID1-1||Index to the Reader. Index should be 1 in this message, meaning this is the first time the device ID1 was HASHed.

NOTE 3: The IDm-n  sent uplink doesn’t have to be sequencial,. For example, the device could send the ID1-1||(Index=1), it can then send ID1-3||(Index=3) after ID1-1||(Index=1).

Step 3: Reader compares the ID1-1 with its HASH table, then confirm this ID1-1 is in its data base.

Step 4: Reader echoes back the ID1-1 to device, following RAN2 procedure.

Step 5: Device checks ID1-1 is correct, use ID1-2 in next message, in which ID1-2 = HASH (ID1-1||(Index =2))

NOTE 4: Reader shall use unused ID for each device for the next paging if there is any.

NOTE 5: Integration of the procedure is to be aligned with inventory procedure as defined by RAN/SA2

### 6.28.3 Evaluation

The impact on the AIoT device and the network are as following:

The AIoT device needs to support to:

1. maintain the root key,
2. decrypt the encrypted device ID using the root key,
3. calculate the HASH (device ID||Index)

The network needs to support to:

1. store the keys for each device ID,
2. paging using encrypted device ID
3. search the HASH table to verify the device ID sent uplink

\*\*\* End of 2nd Change \*\*\*