**3GPP TSG-SA3 Meeting #119e *S3-250055r1***

**emeeting, 13 - 17 January 2025**

**Source: Apple**

**Title: Update solution#8**

**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#8.

# 4 Detailed proposal

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

# 

## 6.8 Solution #8: Mutual authentication for AIoT system

### 6.8.1 Introduction

This solution addresses key issue#5: “Authentication in Ambient IoT service.”

### 6.8.2 Details

Preassumption:

1. AIoT AUSF and AIoT UDM are independent network entities for AIoT system, they can also be collocated with legacy AUSF and UDM, depending on operators’ deployment.
2. The Applacation Function is out of operator domain, which can be the AIoT device manufacture.
3. It is assumed AIoT UDM owns the AIoT device credentials, while Application Function has no access to those credentials.

A screenshot of a computer

Description automatically generated

Step 1. AF sends the authentication request to the AIoT UDM,

NOTE: The authentication request message can be carried in paging message, depending on RAN2/SA2 decision.

Step 2. AIoT UDM generates the RAND, sends the device ID and RAND to AIOT AUSF.

NOTE: AIoT UDM and AIoT AUSF can be collocated.

Step 3. AIoT AUSF sends the device ID and RAND to the AIoTF.

Step 4. AIoTF sends the device ID and RAND to the Reader, Reader includes the device IDs in the paging message.

NOTE: what IDs to be included in paging message will be decided by RAN2.

Step 5. AIoT device calculates the RES using K and device ID and RAND, using HASH function.

Step 6. AIoT device sends the device ID, RES, and random number Counter to Reader in uplink AS message.

NOTE: The message details to be dependent on SA2 decision.

Step 7-8. Reader sends the Authentication Request to AIoT AUSF for authentication.

Step 9. AIoT AUSF sends authentication request to AIoT UDM including the device ID and Counter.

Step 10, AIoT UDM calculates the XRES and network authentication Token. AIoT UDM then sends both values back to AIoT AUSF.

Step 11. AIoT AUSF compares the RES and XRES, if they are equal, AIoT AUSF sends network authentication Token back to Reader in the subsequent messages. Otherwise, the authentication fails.

Step 12-13. the AIoT AUSF passes the authentication result and network authentication Token back to Reader.

Step 14. If the authentication success, the Reader continue with step 15, otherwise, the Reader ceases the authentication procedure.

Step 15. Reader sends the network authentication Token to AIoT devices in DL command message.

Step16. AIoT device verifies if the network authentication Token is correct. If yes, then the authentication of the network is successful, and AIoT device continue with the subsequent UL message. Otherwise, the AIoT device will cease the procedure.

Depending on the device capability, network should decide how often authentication to be performed. If the device capability is sufficient and the authentication is not run every time before the inventory request, the network and the device shall maintain the authentication status of the devices. If the AIoT device capability is too limited, i.e. no storage for the authentication status, the network may need to run the authentication everytime when the inventory is triggered.

Editor’s Note: The synchronization issue is FFS.

NOTE: The solution will need to be aligned with SA2 architecture.

### 6.8.3 Evaluation

The network verifies the AIoT device by comparing the RES and XRES (in step 10), the AIoT device verifies the network by calcualting the token (in step 16).

The device needs to support the capabiltiy of calculating the RES and Token.

The network needs to support the capability of calculating the Token and XRES.

Editor’s Note: Further evaluation is FFS.

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