**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250077-r2**

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

**Source: Xidian, OPPO**

**Title: Pseudo-CR on Resolving ENs for AIoT Security Sol#37**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.5.0**

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

**Comments**

<Proposals, reason for change, abstract, comments if necessary (optional)>

It is proposed to remove the following Editor’s Notes from the solution 37 and revise the solution detail.

* As described in the solution detail update, Then the AIoT device executes the validation procedures of the SQN in the same way as the 5G-AKA, so the following EN can be deleted.

Editor’s Note: How SQN is validated is FFS.

* As this solution is aimed to solve KI#5, and the privacy of device ID in Inventory (i.e., paging) is solved by other solutions, the following EN can be removed.

Editor’s Note: Use of Device ID in Inventory (i.e., paging) and whether it applies to a single or a group of AIoT devices is FFS.

* Since the SA2 has not yet reached a conclusion on the system architecture, including the statement “Editor’s Note: Where to store the AIOT device related information is FFS” in the latest version of 23700-13, we have added the content “It is noted that the UDM can be replaced by a future network function in SA2 used for storing AIoT device related information”, therefore removing the following EN.

Editor’s Note: Impact of using UDM on the network for credential storage and key generation is FFS.

* In order to achieve mutual authentication between the device and the network, the AEAD mode and f2 algorithm are optional. Here, the AEAD mode is dedicatedly achieved by a lightweight algorithm (e.g., AES-GCM), which can provide encryption, integrity protection, and authentication using a single key. And the AEAD algorithm can be used for subsequent secure data transmission. Therefore, the following EN can be removed.

Editor’s Note: How AES AEAD mode is used in the AKA procedure is FFS.

**Proposed Changes**

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

## 6.37 Solution #37: Mutual Authentication Using AEAD for Inventory and Command case

### 6.37.1 Introduction

The solution addresses KI#5. It proposes a mutual authentication using AEAD between AIoT devices and the network. According to the conclusions in TR 23.700-13, the solution makes the following assumptions:

An AIoT device shares a permanent identity (i.e., AIoT Device ID) and root key (i.e., K) with the network side.

### 6.37.2 Solution details

The message flow of this solution is described below:



Figure 6.37.2-1 Mutual authentication for security credentials stored in the UDM

1-2. Third-party AF sends inventory request to the AIoT function through NEF. The request can include an AIoT Device ID to page the device.

3-4. AIoT function generates a fresh nonce and sends the nonce to the AIoT devices through a Reader.

5. AIoT device calculate KAF and authentication parameters.

5.1 AIoT device computes KAF using key derived function. The input parameters include the K, the Device ID and the nonce.

5.2 The device uses f2 or AES algorithm to compute RES. The input parameters include the K, the identity and the nonce.

5.3 Alternatively, the devices can use AEAD algorithm to compute a message authentication code to protect the authenticity of uplink data (i.e. Device ID). The input parameters include the KAF and uplink data (i.e. Device ID).

6. The device sends inventory response (authentication request) including the identity, RES or message authentication code to the Reader.

7. The Reader forwards the response to the AIoT function, including authentication request.

8. The AIoT function sends the authentication request to the UDM, including nonce.

9. The UDM computes KAF and verifies the RES or message authentication code.

9.1 computes KAF using key derived function. The input parameters include the K, the Device ID and the nonce.

9.2 retrieves the SQN and the K according to the ID.

9.3 computes the anonymity key (AK) using f5 or AES algorithm. The input parameters include the K and the fresh nonce.

9.4 computes MAC using f1 or AES function. The input parameters include the K, the SQN fresh nonce and the command message.

10. The UDM sends KAF, AK⊕SQN and MAC to the AIoT function and increases the SQN by one.

11. The AIoT function stores the KAF corresponding to the identity and sends the Command request to the Reader, the message includes AK⊕SQN and MAC.

12. The Reader forwards the Command request to the AIoT device.

13. The AIoT device computes the AK in the same way as the UDM and decrypts the concealed SQN. Then the AIoT device executes the validation procedures of the SQN in the same way as the 5G-AKA (including the re-synchronisation procedures). If the SQN is valid, then it verifies MAC.

14 – 17. Optionally AIoT device sends command response message.

Editor’s Note: Impact of using UDM on the network for credential storage and key generation is FFS.

### 6.37.3 Evaluation

TBD.

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