**3GPP TSG-SA3 Meeting #119 *draft\_S3-245314-r1***

Orlando, US, 11th - 15th November 2024

**Source: Qualcomm Incorporated**

**Title: Addressing the EN in solution #15**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This contribution proposes to address the EN in solution #15.***

# 2 References

[1] TR 38.769

[2] TR 33.713

# 3 Rationale

This contribution proposes solution updates to address the Editor’s Note and add an evaluation text.

Editor’s Note: whether device ID is included is FFS.

Regarding the above Editor’s Note, whether to include device ID in the Command message in step 3 relies on the AS procedure between the Reader and AIoT device as specified in TR 38.769 [1].

According to TR 38.769, the baseline AS procedure for Command is as follows:

* Step A (i.e., A-IoT paging) and Step B (i.e., A-IoT random access procedure, and D2R data transmission) are followed by the Step C (i.e., actual Command and/or response message transmission).

In this case, since the Reader has the information associated with the target AIoT device from step A and step B, the device ID is not required in the Commend message.

Therefore, it is proposed to remove the Editor’s Note and add a following NOTE:

NOTE: Whether device ID is included in the Command depends on the AS procedure specified in TR 38.769 [x]. If the Inventory (i.e., A-IoT Paging, A-IoT random access procedure, and D2R data transmission) is followed by the Command, the device ID is not included in the Command in step 3 as Reader already has the association with the target AIoT device after Inventory.

In addition, it is proposed to add an evaluation text.

# 4 Detailed proposal

It is proposed that SA3 approved the below changes for inclusion in the draft TR [2].

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

## 6.15 Solution #15: End-to-end security protection of command procedure

### 6.15.1 Introduction

This solution addresses key issues #1 and #4. This solution provides a security mechanism for protecting the commands transmitted between an AIoT device and an Application Function (AF) for AIoT services. This solution assumes the AF manages the AIoT device identifier and the corresponding security protection profile. The security protection profile includes a device credential and an algorithm to use to protect the command.

NOTE 1: Device credential types are determined based on each AIoT service and device capability.

The proposed mechanism is also applied to protect the messages exchanged for enable/disable device operation. The security mechanism for protecting the commands is applied when the AIoT device and AF are provisioned with the security protection profile.

### 6.15.2 Solution details



Figure 6.15.2.1-1: End-to-end protection of messages during Command procedure

NOTE 2: The reference architecture and Command procedure described in clause 6.3 of TR 23.700-13 (i.e., solution #3) [4] are used to describe the end-to-end protection mechanism in this solution. The proposed mechanism can be applied to any reference architectures and procedures for AIoT services that require transmissions of messages between AIoT devices and an Application Function.

0. Each AIoT device is provisioned with its AIoT device identifier and security protection profile such as a device credential and an algorithm to use to protect the command. An Application Function (AF) manages the AIoT device identifier and the associated security protection profile.

1. When the AF triggers a Command procedure towards individual AIoT device(s), the AF protects a Command based on the Command Protection Key (CPK) and a freshness parameter. The AF, then, sends a message containing the protected Command to the AIoT Controller.

When the AF triggers a Command procedure towards a group of AIoT devices, it protects a Command based on the Group Command Protection Key (GCPK) and a freshness parameter. Then, the AF sends the protected Command to the AIoT Controller.

NOTE 3: CPK is either derived from the device credential or provisioned on the AIoT device by the AF.

NOTE 4: GCPK, if used, is provisioned on the AIoT devices by the AF.

NOTE 5: Freshness parameter can be a counter, time-based counter or a random number depending on the AIoT service and device capability.

2. The AIoT Controller provides the Command to the selected Reader(s).

3. The Reader sends the Command to the AIoT device(s).

NOTE 6: Whether device ID is included in the Command depends on the AS procedure specified in TR 38.769 [x]. If the Inventory (i.e., A-IoT Paging, A-IoT random access procedure, and D2R data transmission) is followed by the Command, the device ID is not included in the Command in step 3 as Reader already has the association with the target AIoT device after Inventory.

4. Upon receiving the Command, the AIoT device decrypts/verifies the received Command. If the verification is successful, the AIoT device processes the Command.

5. If the AIoT device needs to send a response, it generates a Command Response and protects it based on the CPK and a freshness parameter. The AIoT device, then, sends the protected Command Response.

 In case of Group command, the AIoT device protects the Command response based on the GCPK and a freshness parameter.

6. Upon receiving the Command Response, the Reader sends it to the AIoT Controller with optional Enrichment data such as the location of the Reader if configured by AIoT Controller.

7. The AIoT Controller provides the protected Command Response to the AF.

8. The AF decrypts/verifies the received Command Response based on the CPK and the freshness parameter.

Editor’s Note: The procedure needs to align with SA2.

### 6.15.3 Evaluation

This solution addresses key issues #1 and #4.

In this solution, the Command procedure is protected using the symmetric key between AF and AIoT device.

Editor’s Note: Further evaluation is FFS.

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