**3GPP TSG-SA3 Meeting #119 S3-245311-r1**

Orlando, US, 11 -15 November 2024

**Source: Ericsson**

**Title: Addressing ENs in Solution#29 to KI#3**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***This document addresses editor’s notes in Solution #29 in TR 33.713***

# 2 References

None

# 3 Rationale

This solution assumes that SA2 specifies a paging message in such a way that an AIoT device can recognize if the paging message is meant for the AIoT device. The exact content of the paging message is dependent on SA2 specification. We add the above reasoning in a note. Therefore, we propose to remove the following editor’s note:

Editor’s Note: The content of the paging message and how the device decides to respond to the paging message based on the content of the paging message is FFS.

AICI is not stored in the network. Instead, the network decrypts AICI. A device accepts an AICI only if it is computed by the legitimate home network --- hence a device cannot have an AICI that the network won’t recognize. Therefore, the question about AICI synchronization in the network is not relevant. We add the above reasoning in a note. Therefore, we propose to remove the following editor’s note:

Editor’s Note: Synchronization of AICI is FFS

The entity that computes and decrypts AICI is the entity that stores the shared primary key K of the device. SIDF/UDM is shown as an example in this solution. We add the above as a note. Therefore, we propose to remove the following editor’s note:

Editor’s Note: Whether AICI is to be computed and decrypted in SIDF/UDM is FFS

We add a note that says the solution requires AIoT devices to have the capability to update and store AICI. Therefore, we propose to remove the following editor’s note:

Editor’s Note: Whether AIoT device can update and store AICI is FFS

# 4 Detailed proposal

**\*\*\*\*** START OF CHANGE **\*\*\*\***

## 6.29 Solution #29: Providing a network-computed AIoT concealed device identifier (AICI) to an AIoT device

### 6.29.1 Introduction

This solution addresses KI#3: Privacy by protecting AIoT device identifiers.

### 6.29.2 Solution details

The solution proposes a method for the 5G network to compute a AIoT Concealed Device Identifier (AICI) and provide the SUCI to the AIoT device in a command message. Once an AIoT device is identified, e.g., after a successful completion of inventory procedure, the network can send a command message on the downlink channel to the AIoT device. In the downlink command message, the network includes an AICI, which is computed based on the long-term identifier of the AIoT device using the public key of the network. The downlink command message is both confidentiality and integrity protected using keys derived from a shared key between the network and the AIoT device. Figure 6.29.2-1 presents a high-level message flow of the solution.



Figure 6.29.2-1: Procedure for delivering a AICI to an AIoT Device

The figure is self-explanatory, therefore, the steps are not explained step-by-step. Exact content of the messages exchanged, and details about authentication challenge, computing response to the challenge, and deriving the keys Kenc and Kint are not described because these details have to be adjusted with the authentication protocol that is finally agreed.

NOTE 1: If the AIoT device does not have a network-computed AICI, for example, in the very first time of the device’s life cycle, then the AIoT device computes AICI using null scheme. This happens only in the beginning. To avoid using null scheme in the first time, a network can choose to provision every AIoT device with a network-computed AICI before they are handed out to their users.

Editor’s Note: The content of the paging message and how the device decides to respond to the paging message based on the content of the paging message is FFS.

NOTE 3: AICI is not stored in the network. Instead, the network decrypts AICI. On the other hand, a device accepts an AICI only if it is computed by the legitimate home network — hence a device cannot obtain an AICI that the network won’t recognize. Therefore, the question about AICI synchronization is not relevant.

Editor’s Note: Whether AICI is to be computed and decrypted in SIDF/UDM is FFS

NOTE 5: The solution requires AIoT devices to have the capability to update and store AICI.

### 6.29.3 Evaluation

TBD

**\*\*\*\*** END OF CHANGE **\*\*\*\***