**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250058-r9**

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

**Source: OPPO, Huawei, HiSilicon, Apple,…**

**Title: Pseudo-CR on Conclusion on KI#5 AIoT Authentication**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.5.0**

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

**Comments**

It is proposed to agree the conclusion on KI#5 of AIoT authentication.

There are 16 solutions for KI#5 AIoT authentication in 33713 v 050. In order to make progress on conclusion for KI#5, observations and proposals for authentication solutions are listed as following

1. **Observation 1**: Direction of authentication: most of the authentication solutions proposed mutual authentication instead of one-way authentication. Therefore, it is proposed to agree mutual authentication as baseline for normative work.
2. The number of mutual authentication solutions is TWELVE: #6, #7, #8, #10, #11, #12, #13, #32, #35, #36, #37, #39.
3. The number of network authenticating device only solutions is FOUR: #4, #9, #38, #42.
4. **Observation 2:** Network element performing authentication: All of SIXTEEN solutions proposed to use network element to perform authentication. Therefore, it is proposed to agree network layer authentication as baseline for normative work.

Which exact network element will store and process subscription data of AIoT device is pending on SA2 agreement.

* 1. AIoT Authentication Function/ Authentication Server: #4, #7, #32, #42
  2. AIoT Controller: #6
  3. AIoT UDM/AUSF: #8, #11, #12, #37, #39
  4. AIoT F/NF: #9, #13, #35, #36, #38
  5. AAA-S: #10

1. **Observation 3:** Authentication credential: Twelve out of SIXTEEN proposed to use pre-provisioned shared key between AIoT device and network for authentication. Therefore, it is proposed to agree to use pre-provisioned shared key between AIoT device and network for authentication.
   1. Root Key/K/ pre-provisioned key: #4, #7, #8, #9, #11, #12, #13, #32, #35, #37, #38, #39, #42
   2. Derived Kaiot: #6
   3. AIoT credentials: #10
   4. Not clear: #36
2. **Observation 4:** All these solutions propose Challenge-Response based procedure to perform authentication.
3. **Observation 5:**  fresh parameter, ELEVEN out of SIXTEEN proposed to use random number from network side for authentication. Therefore, it is proposed to agree to use random number from network side for authentication.
   1. RAND/NONCE from network side: #4, #7, #8, #9, #11, #12, #13, #35, #37, #38, #39
   2. RAND/NONCE from device side in addition of a): #4, #9, #35, #39
   3. Counter: #6,
   4. freshness parameter: #42
   5. L1 parameter: #32,
   6. Not clear: #10, #36

**Proposed Changes**

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

7 Conclusions

## 7.x Conclusion on KI#5

1. The credential (including device ID and authentication credential) for AIoT device authentication can be owned by an operator or by a third party. The principles for device ID management are concluded in 8.2.1 in TR 23.700-13 [4].

2. For operator managed AIoT devices, the following principles are taken as the conclusion for KI#5:

Inventory-only Procedure:

* For inventory-only procedure, One-way (i.e., the 5G network authenticates the AIoT device) shall be supported.

NOTE X: Details of the one-way authentication procedure (e.g., parameter(s) used, whether one-way authentication can be implicit or not, etc.) are to be resolved during normative phase.

Inventory and Command Procedure:

* Mutual authentication between the AIoT device and the 5G network shall be supported.
* The authentication procedure is based on a challenge-response mechanism.

NOTE Y: Details of the mutual authentication procedure (e.g., parameter(s) used for the 5G network to authenticate the AIoT device and for the AIoT device to authenticate the network) are to be resolved during normative phase.

The credential is stored with AIoT device information.

3. Additional considerations during normative phase:

NOTE 1: Where to store the AIoT device subscription will be based on SA2 and SA3 coordination.

NOTE 2: Which case (i.e., inventory only, or inventory and command) will be indicated in Service type information by AF to the MNO (clause 8.3.5 of TR 23.700-13 v120 [4]).

NOTE 3: The selection of one-way or mutual authentication is a deployment choice and based on a static configuration/implementation in the device and core.

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