**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250012**

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

**Source: Sony**

**Title: KI#5, Conclusions**

**Document for: Approval**

**Agenda item: 5.9**

**Spec: 3GPP TR 33.713**

**Version: 0.5.0**

**Work Item: FS\_AIOT\_Sec**

**Comments**

The Ambient IoT Check point at TSG SA#106 resulted in Way Forward in SP-241980.



The Way Forward includes important aspects on how to focus the work in Q1 to reach conclusions that can be implemented during the normative phase during Q2 and Q3, 2025.

The most important guidance is to focus the work on device type 1 (the most constrained device type) and topology 1 (base station reader), as this is what RAN will specify in Rel-19 according to approved WID in RP-243326.

**Proposal 1:** As device type 1 is very constrained it can be concluded that these devices cannot use an USIM. Solution 11, 12 and 39 cannot be considered.

In TR 33.713 v.0.5.0 there are 16 solutions (incl 11,12 and 3) documented related to KI#5 Authentication in Ambient IoT service.

It is important that both the AIoT device and the network can authenticate each other. A network must at least be able to authenticate a response from an AIoT device as only responses from AIoT devices with valid credentials should be handled. Likewise, the AIoT device must be able to authenticate that a command message originates from a trusted source i.e., a trusted network operator.

**Proposal 2:** Authentication for AIoT device type 1 is done by authenticating the received message by both the network and AIoT device.

Rel-19 will support two types of services: Inventory and Command. The Inventory service can be viewed as paging a specific device or a group of devices. The responding devices is recorded by the Reader performing the Inventory. RAN2 assumption is that the paging message includes ID(s).

**Proposal 3:** Not to add an authentication code or HASH to the paging message (Inventory request).

For the Command message it is essential that the device can trust the sender of the command that will receive the response and/or to act based on the command received. Therefore, the device should be able to verify the authenticity of the command message.

**Proposal 4:** Add an authentication code or HASH to the command message.

**Proposal 5:** For the responses to a Inventory Request (paging message) the device may add an authentication code or HASH. For the responses to a Command message, the device shall add an authentication code or HASH to allow the network to verify the authenticity of the response message received.

As AIoT device type 1 is very constrained, the focus should be on the solutions that suggests low complexity operations for the device supporting the proposals in proposal 3-5.

**Solution Investigation (mapped to KI#5 in table 6.1-1)**

Solution 4: A Nonce is added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedures in 6.4.2 can be considered.

Solution 6: A MAC is added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedures in 6.6.2 can be considered, but the solution has many open ENs.

Solution 7: Dedicated Authentication Request (Command to authenticate the device). The solution has many open ENs.

Solution 8: Dedicated Authentication Request (Command to authenticate the device), triggered by the AF.

Solution 9: A Nonce is added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedures in 6.9.2 can be considered.

Solution 10: A optional Authentication container is added to the paging message, which is not in line with RAN 2 assumption. However, it is said to be optional – meaning not needed. The rest of the procedure in 6.10.2.2 can be considered but are the computational tasks to be executed by the device light weight?

Solution 13: A Nonce, SQN and MAC added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedure in 6.13.2 can be considered but are the computational tasks to be executed by the device light weight?

Solution 32: Use L1 radio channel measurements to generate RAND used for authentication. Several ENs are captured indicating that this concept needs more work especially in RAN1.

Solution 35: A Nonce is added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedure in 6.35.2 can be considered but are the computational tasks to be executed by the device light weight?

Solution 36: Suggest a dedicated security domain for AIoT functions in the network.

Solution 37: A Nonce is added to the paging message, which is not in line with RAN 2 assumption. The optional Command response message cannot be authenticated by the network.

Solution 38: Two RANDs, and the command PDU are added to the paging message, which is not in line with RAN 2 assumption. The rest of the procedure requires the input in the paging message to be conducted.

Solution 42: The device selects a preconfigured Nonce from a list of Nonce values and encrypts the device ID. The encrypted device ID is used to authenticate the response message. Some security concerns are captured in ENs related to the preconfigured list of Nonce values.

**Observation:** Proposal 3-5 suggests that Ambient IoT authentication is done by authenticating the message. This implies that part of KI#4 Protection of information during AIoT service communication i.e., “ensure integrity and/or anti-replay of information for AIoT services.”. Solutions addressing KI#4 should therefore also be investigated.

**Solution Investigation (mapped to KI#4 in table 6.1-1)**

Additional solution not overlapping with KI#5 are 14, 15, 33 and 40.

Solution 14: Propose to use one time ID for Inventory which only authorized device and network can derive. For Command MAC is proposed to be used.

Solution 15: Propose to encrypt the Command and if device can decrypt the command message it can also verify the message.

Solution 33: Use L1 radio channel measurements to generate L1-key used for generating session keys Kiot which is then used to protect the command message. Several ENs are captured indicating that this concept needs more work especially in RAN1.

Solution 40: Propose that the device does not authenticate the command message.

**Observation:** There are several solutions that are quite similar, but differentiate in certain aspects e.g. MAC or HASH, freshness parameter provided over-the-air or not, Session key is derived or shared key is used.

**Proposal 6:** Conclude that the normative work for Authentication can be based on conclusions on KI#4 related the message integrity/authentication. Select a low complexity solution for KI#4.

**Proposed Changes**

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

## 7.x Conclusions on Key Issue #5

For key issue #5 (Authentication in Ambient IoT service), it is concluded that for Ambient IoT device type 1 in Rel-19 the authentication will be based on message authentication and integrity protection as concluded for KI#4 in clause 7.4.

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