**3GPP TSG-WG SA2 Meeting #167 *S2-2502320***

**Athens, GR, 17th Feb – 21st Feb, 2025 (revision of S2-2501969)**

**Source: Huawei, HiSilicon**

**Title: Resolve the editor’s notes related to security aspect**

**Document for: Approval**

**Agenda Item: 19.14.1**

**Work Item / Release: FS\_AmbientIoT / Rel-19**

*Abstract: this pCR proposed to resolve the editor’s notes related to security aspect.*

# 1. Introduction/Discussion

In TR 23.700-13 v1.3.0, there are three editor’s notes related to security aspects:

|  |  |
| --- | --- |
| SA2 Key issue | Description of editor’s notes |
| Key issue 2 | Whether the temporary ID in the AIoT NAS layer is required for the privacy protection is FFS and is pending SA WG3 decision |
| Key issue 1 | Whether and how the AIoT Device ID privacy protection and ID authentication is done will be concluded by SA WG3 |
| Key issue 3 | Whether and how the A-IoT Device Identification information will be security protected will be concluded by SA WG3 |

It is summarized the above editor’s notes are related with two key issues in SA3 study (TR 33.713):

* SA3 TR key issue#3: Privacy by protecting AIoT device identifiers (yellow highlight)
* SA3 TR key issue#5: Authentication in Ambient IoT service (cyan highlight)

Assuming the key issue discussion on privacy will be concluded by SA3, SA2 will align with SA3 TR conclusions for AIoT Device security including AIoT Device ID privacy protection, in the normative phase.

However, SA2 has not discussed “Authentication” in study phase, which should be under SA3 working scope.

In the SA2#166 ad-hoc e-meeting, it was concluded not to pursue the feature on temporarily enable/disable the AIoT device, it is proposed to update the TR conclusion clause 8.3.2 accordingly.

# 2. Text Proposal

It is proposed to capture the following changes vs. TR 23.700-13, v1.3.0.

\* \* \* \* First change \* \* \* \*

### 8.1.1 General

Key issue #1 includes the following aspects:

- System architecture identified along with the solutions for KI#2 and KI#3.

Key issue#2 aspect on "Ambient IoT Device subscription management" and key issue#3 aspect on "Ambient IoT service exposure" is considered in this clause.

In this release, normative work will take place for Topology 1 and no normative work will take place for Topology 2.

The following aspects common for Topology 1 and Topology 2 are concluded as principles for normative work:

1. A new core network function is introduced to support Ambient IoT (e.g. AIOTF) service for both the topology 1 and topology 2. The AIoTF performs the following functionality.

a. The AIOTF registers itself in the NRF with its NF profile, this is to enable the discovery of AIOTF instances e.g. by an NEF. The NF profile at least includes the AIOTF ID/address, NF type, information used to allow the NEF to discover AIOT instances, e.g. based on the target area information in AF request. Other details of the NF profile, if needed, will be completed in normative phase.

b. For topology 1, the AIOTF selects AIOT RAN nodes and optionally a list of the BS readers. For topology 2, the AIOTF selects the UE readers (e.g. candidate or final UE readers) and provides the selected UE Reader list to the RAN.

NOTE 1: Providing the UE Reader list to the RAN only applies to the RRC-based option.

For topology 1, NGAP is terminated at an AIOT RAN node. An AIOT RAN node that supports one or more BS readers, may report its supported BS reader information e.g., BS reader IDs and their corresponding service areas. The OAM may configure the AIOTF with BS Reader information including e.g., their corresponding service area when the BS Readers are integrated in the network.

NOTE 2: Whether RAN3 will specify BS reader information (e.g. BS reader ID, service area) reporting to AIOTF over NGAP depends on RAN3 decision and if so SA2 may include this feature in SA2 specifications.

NOTE 3: If the request from the AIOTF to the AIOT RAN does not include a BS reader list, then AIOT RAN can use all available BS readers.

NOTE 4: The BS reader’s service area needs to coordinate with RAN WG(s).

c. The AIOTF receives an AIoT service request from the AF and triggers the BS/UE Readers to perform AIoT service operations towards the AIoT Devices(s).

d. The AIOTF aggregates the service operation results (including the removal of the duplicated devices records) from BS Readers and UE Readers and sends to AF.

e. The AIOTF may provide the following assistance information to AIoT RAN/UE Reader:

- AIoT service type (e.g. Inventory, Command);

- approximate number of AIoT devices based on AF request;

- approximate D2R message size based on AF request.

NOTE 5: If there are multiple Readers selected for the AIoT Service, the AIOTF may provide the approximate number of AIoT devices to each Reader based on implementation.

NOTE 6: The approximate D2R message size considering the overhead of AIoT Device NAS layer will be determined later in cooperation with CT WG1 and SA WG3.

NOTE 7: Further assistance information can be added during the normative phase and in cooperation with other WGs if necessary.

Editor's note: For RRC based solution of topology 2, whether the aggregation can be performed by the RAN is FFS and coordination with RAN WGs is needed.

Editor's note: How the aggregation can be done is FFS.

f. When the AIOTF sends an operation request to a UE Reader or BS Reader (via AIOT RAN), a response and one or more reports with the results of the AIoT service operation is returned to the AIOTF with the results of the AIoT service operation, and the AIOTF needs to correlate the results to a given operation request. The AMF (if used to route the requests) additionally provides an AIOTF identifier with the request from the AIOTF which is returned with the response(s) related to the request, so the AMF can be routed back the requesting AIOTF.

2. A Permanent AIoT Device ID is stored in the AIoT Device and the network or a Credential Holder's AAA server. The AIOTF checks whether the AIoT Device ID from AIoT Device has a subscription and retrieves.

NOTE X: SA2 will align with SA3 TR conclusions for AIoT Device security including AIoT Device ID privacy protection, in the normative phase.

3. The AIoT Device does not distinguish whether the connectivity topology is Topology 1 or Topology 2, nor the transport used by the AIoT Reader.

NOTE 8: The AIoT device is also agnostic to the potential different architectures if more than one architecture is concluded for both the topology 1 and topology 2.

4. AIoT Device NAS protocol is supported between the AIoT Device and the AIOTF. The AIoT Device NAS layer supports Inventory Response and Command (e.g. Read and Write) Request and Response.

5. The AIOTF may store and manage the AIoT device related information (also known as device context information) locally that includes e.g., the AIOT device permanent ID, the last known reader information of the AIoT device. The last known reader information can be used to support the AIOTF to select the serving reader to forward the message towards the specific AIoT device(s).

NOTE 9: The storage of security related information at the AIOTF is up to the coordination with SA WG3 later.

\* \* \* \* Second change \* \* \* \*

### 8.2.1 Identifier and Identification Management

The following aspects and principles are considered and agreed for the interim conclusion on Identifier and Identification Management.

The following principles are agreed for Identifier and Identification Management:

- An Ambient IoT Device is configured with a permanent Ambient IoT Device Identifier which can be assigned by an operator or by a third party. The Identifier is used to identify Ambient IoT Device and locate the corresponding authentication server.

NOTE 1: How to configure Ambient IoT Device with the permanent Ambient IoT Device Identifier is out of 3GPP scope.

The permanent Ambient IoT Device Identifier includes the following information:

1) Part1information:

- The ID type, including

- information indicating whether the network identifier is included or not.

- information indicating whether information used to identify a 3rd party is included or not.

- the Part2 type indicating EPC or the other format.

- A network identifier (i.e. MCC+MNC and/or NID), when the ID includes the network identifier.

- Information used to identify a 3rd party when the ID includes the information used to identify a 3rd party.

2) Part2 information:

- The information (e.g. EPC or others) used to distinguish different Ambient IoT Devices within the scope identified by the Part1 information.

Editor's note: Part2 information for the operator assigned and 3rd party assigned ID needs further study.

NOTE 3: The coding for the above information is left to stage 3.



Figure 8.2.1-1: The example of Operator allocated ID

For operator allocated Part 1 information, the network identifier is mandatory and can be used to index the authentication server or not. If it is not used to index the authentication server, the ID may further include the information used to identify a 3rd party. The third party may be the credential holder or not. If it is not the credential holder, the network should be provided with third party related context including the information used to locate the authentication server.



Figure 8.2.1-2: The example third party allocated ID

For third party allocated Part 1 information, the network identifier is not needed. The third party may be the credential holder or not. If it is not the credential holder, the network should be provided with third party related context including the information used to locate the authentication server.

NOTE 4: Within each type of ID, the length of Part 1 is fixed (i.e. the length of ID type, the Network Identifier (if present) and the Information used to identify a third party (if present) are fixed) and the length of Part2 is dynamic. The detail is left to stage 3.

With the above information, the AIoT device ID is globally unique.

NOTE X: SA2 will align with SA3 TR conclusions for AIoT Device security including AIoT Device ID privacy protection, in the normative phase.

\* \* \* \* Third change \* \* \* \*

### 8.3.4 Principles on the procedures to support AIoT services

To support the services provided by 5GC and the NEF exposure of those AIoT services, the following procedures are supported:

- Inventory Procedure.

- Command Procedure, to e.g. transfer AF AIoT Data to/from AIoT Device(s) as AIoT specific NAS messages.

There are requests that are used from the AIOTF towards the Reader and responses from the Reader to the AIOTF. The routing of the request and response messages and their encoding depends on the topology and transport to the Reader (see KI#1).

All the procedures follow have the following steps:

1. The AF makes a service request to the NEF, including parameters as defined in clause 8.3.5.

2. The NEF determines an AIOTF for the requested operation, and invokes a new service operation on the AIOTF.

3. For the requested operation the AIOTF:

1). Performs initial reader selection by either:

- The AF provide information to identify readers to include in the initial reader selection network. The information can identify multiple or an individual Reader.

NOTE 1: Which readers are identified by the information from the AF is up to the network deployment, configuration or implementation.

- If a single UE Reader ID is provided by the AF via the NEF for the operation, then that is used as the selected Reader.

- If reader selection information or UE Reader ID is not provided, then how the AIOTF determines which readers to use is based on implementation. The AIOTF may be e.g. preconfigured with which readers to use, or take the requested target AIoT Devices last known location into account, etc.

If no readers can be selected then the request is rejected.

2). Determines AIoT Device Identification information based on the information from the AF, to be included in the paging message on the AIoT radio interface to find the AIoT Devices. AIoT Devices compare the AIoT Device Identification information with their own AIoT Device Identifier (part of or full AIoT Device Identifier) to determine whether respond to the paging message.

NOTE X: SA2 will align with SA3 TR conclusions for AIoT Device security including AIoT Device ID privacy protection, in the normative phase.

3). Determines Reader Assistance information required for the operation used to the Reader, taking into account assistance information from the AF.

4). Constructs a request for an Inventory operation using the determined A-IoT Device Identification information page the AIoT Devices, and a correlation identifier for the AIOTF to correlate the inventory responses to the request. The Inventory request is routed to the Readers determined by the initial reader selection.

See clause 8.1 for how to provide the request to a Reader.

5). The Reader executes the inventory request, reporting AIoT specific NAS message responses from the AIoT Device to the AIOTF, including its Reader ID and correlation identifier from the AIOTF. The Reader may aggregate results from multiple AIoT Devices in the responding messages. The AIOTF can determine which request the results are for using the correlation identifier.

6). The AIOTF may, depending on the information within the AIoT Device identifier, obtain subscription-like information from either:

- the serving network performing the operation (either as identified by a AIoT Device Identifier or operator policy to check it been provided with information for a specific AIoT Device), or

- another network as identified by a AIoT Device Identifier, or

- A third party as identified by a AIoT Device Identifier.

7). Checks if the AIoT Device is subscribed.

NOTE 2: Whether and how AIOT Device Identifiers are verified depends on SA WG3.

8). If the operation is a command operation, the AIOT generates a request, including an AIoT specific NAS message for the command, along with any additional information required by the Reader to execute the command, and a correlation identifier to determine the destination of command responses. The request is then routed to the Reader. The Reader executes the command, passing the AIoTF specific NAS message to the AIoT Device and collecting any AIoT specific NAS responses. The AIoT specific NAS responses are then routed back to the AIOTF.

NOTE 3: Whether and how security protection is applied to the AIoT specific NAS message send to the AIoT Device and the response AIoT specific NAS message from the AIoT Device depends on SA WG3.

9). Provide the results of the operation to the NEF. Results from multiple AIoT Devices may be included/aggregated in the service response(s).

4. Provide the results of the operation from the NEF to the AF.

\* \* \* \* Fourth Change \* \* \* \*

8.3.2 AIoT services supported by the 5GC

The following Ambient IoT services are agreed to be supported by the 5GC, which apply to both topology 1 and topology 2:

- Inventory: Request to perform an inventory operation.

- Read: Request to read information from an AIoT Device.

- Write: Request to write information to an AIoT Device.

- Disable: Request that an AIoT Device has its capability to transmit RF permanently disabled.

NOTE 1: The security aspect of Disable is to be concluded by SA WG3.

NOTE 2: The temporarily disabling and enabling of AIoT devices did not reach conclusion and will therefore not be supported in release 19.

\* \* \* \* End of changes \* \* \* \*