**3GPP TSG-WG SA2 Meeting #166-AHe *S2-2501250***

**E-meeting, 20th Jan – 24th Jan, 2025 (revision of S2-2500925r02)**

**Source: Huawei, HiSilicon**

**Title: Editor’s Notes resolutions during the normative phase or future releases (Cat-2 & Cat-3 ENs)**

**Document for: Approval**

**Agenda Item: 19.14.1**

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

*Abstract: Conclusion update to resolve the related ENs identified as Cat-2 and Cat3 editor’s notes in the TR.*

# 1. Introduction/Discussion

## 1.1 Overview

There are a few of Editor’s Notes captured in the TR conclusion, which can be solved based on the WID scope of Ambient IoT in Release 19. Moreover, some Editor’s Notes are related to the detailed aspect which can be further determined during normative phase with coordination with other WGs if needed. Therefore, this pCR analyses the Editor’s Notes in the TR conclusion and resolves them.

## 1.2 Key Issue 1 Editor’s Notes

Editor's note: Final conclusions are assumed to be taken in coordination with RAN WGs.

Based on plenary outcome, the scope of R19 Ambient IoT Work Item has been determined. This EN can be removed and the scope of the normative phase is captured in the TR conclusion. Additional text is added to clarify that topology 2 is pursued in this release.

Editor's note: The details of the NF profile are FFS.

The NF profile in the NRF is used by the NEF to discover the instances of AIOTF. The similar parameters for NF discovery can be introduce to help discover AIOTF instances, like NF type, NF Address/ID, Reader Area ID/geographic area like service area info. etc.

Clarify that NF profile is used to discover the AIOTF instances and details of the NF profile can include the NF address/ID, NF type, service area information (e.g., Reader Set/Area ID, geographic area), and the details will be determined during the normative phase.

Editor's note: Whether and how the AIoT Device ID privacy protection and ID authentication is done will be concluded by SA WG3.

This is the scope of SA3 and can further coordinate and keep aligned with SA WG3 during normative phase.

Editor's note: How addressing works for UL traffic (i.e. how the BS Reader identifies the appropriate AMF to which to forward UL messages) in the indirect path via AMF is FFS.

Based on the TR conclusion in clause 8.1.1 and clause 8.3.4, the AIOTF will generate a correlation identifier which is used to correlate the results to a given operation request. The correlation identifier will be sent to AIOT RAN which will be sent back to AIOTF when reporting the responses to requested operations. In other words, AIOT RAN will be able correlate the correlation identifier with the AIOTF. In the indirect architecture, AIOT RAN will also be provided with an AIOTF identifier as described in clause 8.1.1, so it can correlate the correlation identifier with the AMF and AIOTF so that the AIOT RAN can route the UL traffic to the appropriate AMF. The detailed call flow can be specified during normative phase and can be converted to a NOTE and aligned with RAN during the normative phase.

## 1.3 Key Issue 2 Editor’s Notes

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

Part 2 information is used to identify a specific AIoT Device within the scope of Part 1 information. Considering there may be thousands of different industries and different industries may have different format to identify a specific object. Therefore, it would be difficult to define in the specification the subdivision of part 2 information. Hence, based on such consideration, it is recommended that the detail format should leave to implementation to provide flexibility to the operator or 3rd party (i.e. the part 1 scope). Therefore, the EN can be removed and add a NOTE to clarify that the detail of part 2 information is based on operator or 3rd party implementation.

Editor's note: Whether the temporary ID in the AIoT NAS layer is required for the privacy protection is FFS and is pending SA WG3 decision.

This is the scope of SA3 and can be further aligned with SA WG2 during normative phase.

Editor’s note: SA WG2 will align security related materials in subscription data with SA WG3 decision later.

This is the scope of SA3 and can be further aligned with SA WG2 during normative phase.

Editor’s note: Items within the subscription data for 3rd party AF need to be figured out later.

The subscription data for a 3rd party AF is used by the AIOTF together with SLA and operator policy at NEF to perform authorization of the AF request. This authorization can be check at three aspects: 1) Check whether the AF is authorized for the requested device operation; 2) Check whether the AF is authorized for the requested UE reader or target area; 3) Check whether the AF is authorized for the requested target AIoT device(s).

Clarify that the subscription data for 3rd party AF can be used to check requested device operation, the requested target area or the requested target AIoT device(s). Items within the subscription data for 3rd party AF can be figured during normative phase.

## 1.4 Key Issue 3 Editor’s Notes

Editor's note: Additional conclusions are FFS.

This EN can be removed directly since the scope of R19 Ambient IoT Work Item has been determined during SA and RAN plenary.

Editor's note: NEF event exposure aspect is FFS.

The NEF event exposure is used to receive AIoT Service Requests from a third party to perform operations towards AIoT Devices and provide the results to the third party. The AIoT Service can include several Service Operations such as Inventory, Read, Write, Permanent Disable and Notify to support different types of AIoT Service and result notification. It is clarified that these services operations will be defined.

Editor's note: Whether and how the A-IoT Device Identification information will be security protected will be concluded by SA WG3.

This is the scope of SA3 and can be further aligned with SA WG2 during normative phase.

# 2. Text Proposal

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

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

## 8.1 Conclusion on Key Issue #1

### 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 the BS readers or AIOT RAN nodes. 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.

Editor’s note: Whether and how AIOTF selects BS readers or AIOT RAN nodes in topology 1 needs coordination between SA WG2 and 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 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.

Editor's note: Other assistance information may be added later if necessary.

Editor's note: Further information on AIoT service type may be determined later in cooperation with RAN WGs.

NOTE 2: 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 3: 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.

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.

Editor's note: Whether and how the AIoT Device ID privacy protection and ID authentication is done will be concluded by SA WG3.

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 4: 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.

Editor's note: It is FFS whether to support any other messages besides Inventory Response, Command (e.g. Read and Write) Request and Response over AIoT Device NAS layer.

5. The network may manage the AIOT device related information (e.g. device context information), includes the AIOT device permanent ID, and optionally the last known reader information.

Editor’s note: How this AIOT device related information is used is FFS.

Editor’s note: Where to store the AIOT device related information is FFS.

### 8.1.2 Architecture to Support Topology 1

#### 8.1.2.1 General

The principles and aspects in this clause are agreed to support Topology 1:

- The new core network function (AIOTF) is introduced to support Ambient IoT functionality, described in clause 8.1.1, with the following features for topology 1:

- Send requests that trigger BS Reader(s) (via AIoT RAN) to perform AIoT operations, either directly or via an AMF.

NOTE 1: It is assumed AIoT RAN supports Ambient IoT specific functionalities. There is no assumption about whether the AIoT RAN (i.e. BS Reader) also has any gNB functionality for NR-Uu or not.

NOTE 2: NGAP is used when the AIOTF directly communicates with the AIOT RAN (i.e. over the Nx reference point) or indirect communication with AIOT RAN via an AMF (i.e. over the N2 reference point).

NOTE 3: It is assumed Ambient IoT services can be deployed independently from existing deployments.

NOTE 4: It is not expected a deployment will use both direct communication between AIOT RAN and an AIOTF and indirect communication between AIOT RAN and an AIOTF via an AMF. The deployment choice can be based on, for example, using a direct communication path for a local deployments.

- The signalling transport for NGAP at the A-IoT RAN node is SCTP/IP.

#### 8.1.2.2 AIOT RAN and the AIOTF communicate directly

When a AIOT RAN and the AIOTF communicate directly:

- The AIOTF communicates with a AIOT RAN via a direct interface reference point Nx.

- Figure 8.1.2.2-1 below shows the aspects related to Topology 1 (direct path) architecture in reference point representation architecture with other NFs removed.



Figure 8.1.2.2-1: Non-Roaming 5G System Architecture (Direct Path)

- Figure 8.1.2.2-2 below shows the aspects related to Topology 1 (direct path) architecture in reference point representation with other NFs removed.



Figure 8.1.2.2-2: Non-Roaming 5G System Architecture in reference point representation (Direct Path)

NOTE 1: NGAP used over Nx reference point will support procedures and information to be exchanged as specified by RAN WG2, RAN WG3 and SA WG2.

NOTE 2: The protocol stack used between the AIoTF and the AIOT RAN will be concluded by RAN WG3.

- Figure 8.1.2.2-3 below shows the aspects related to Topology 1 (direct path) protocol stack between the AIOT RAN and AIoTF.



Figure 8.1.2.2-3: Example Protocol Stack between AIOTF and AIoT Device for Topology 1 (Direct Path)

NOTE 3: Whether AIoT Reader Control is transported by NGAP or is part of the NGAP protocol will be determined by RAN WG3.

#### 8.1.2.3 AIOT RAN and the AIOTF communicate indirectly via an AMF

When AIOT RAN and the AIoTF communicate indirectly via an AMF:

- The AIoTF connects with AIOT RAN via an AMF. NGAP over the N2 reference point between the AIOT RAN and AMF supports Ambient IoT services including delivery of inventory/command messages.

NOTE 1: If network isolation is required an AMF instance is deployed for supporting the AIOTF communication with AIOT RAN.

- NGAP between AIOT RAN and the AMF is enhanced to support Ambient IoT Services.

NOTE 2: The details of the enhancements will be concluded by RAN WG3.

- The AMF shall be enhanced to support:

- On the Nz reference point, the AMF supports Services which are used by an AIoTF for Ambient IoT Operations e.g. to send AIoT requests towards AIOT RAN and to receive AIoT responses from the AIOT RAN.

- On the N2 reference point, the AMF supports sending AIOT information to the AIOT RAN (e.g. operation requests) and receiving responses from the AIOT RAN.

- The AMF routes the AIoT messages between the AIOT RAN (over N2 reference point) and the AIOTF (over Nz reference point).

NOTE 3: Whether to enhance an existing service or define a new service will be determined in the normative phase.

- Figure 8.1.2.3-1 below shows the aspects related to Topology 1 (indirect path via AMF) architecture in reference point representation with other NFs removed.



Figure 8.1.2.3-1: Non-Roaming 5G System Architecture (indirect Path via AMF)

- Figure 8.1.2.3-2 below shows the aspects related to Topology 1 (indirect Path via AMF) architecture in reference point representation with other NFs removed.



Figure 8.1.2.3-2: Non-Roaming 5G System Architecture in reference point representation (indirect Path via AMF)

- Figure 8.1.2.3-3 below shows the aspects related to Topology 1 (indirect path via AMF) protocol stack between AIOT RAN and AIoTF.

- AIoT Data represents information exchanged between the AIoT Device and AF (application specific content) and AIoT Reader Control represents the requests and responses between the AIOTF and AIOT RAN.



Figure 8.1.2.3-3: Example Protocol Between AIOTF and AIoT Device for Topology 1 (indirect Path via AMF)

NOTE 4: Whether AIoT Reader Control is transported by NGAP or is part of the NGAP protocol will be determined by RAN WG3.

NOTE 5: UL traffic is routed based on an AIoT correlation identifier (i.e. AIOT-RAN identifies the appropriate AMF to which to forward UL messages base on the association between AIoT correction identifier and the AMF); details will be determined during normative work.

### 8.1.3 Architecture to Support Topology 2

#### 8.1.3.1 General

The following principles apply:

- Architecture: Two architecture options will be specified for Topology 2:

- User-plane option as defined in clause 8.1.3.2.

- RRC-based option as defined in clause 8.1.3.3.

- Subscription aspects:

- The UE subscription in the UDM will be extended with UE Reader subscription information, which consists of the following:

- information indicating whether the UE is allowed to operate as a UE Reader.

Editor’s note: Additional subscription information, e.g. validity information, for the UE Reader is FFS.

- UE Reader subscription information is available to AMF and AIoTF.

- If AMF receives, as part of the subscription information, the indication that the UE is authorized to operate as a UE Reader, then AMF informs NG-RAN that the UE is authorized to operate as a UE Reader.

Editor’s note: Whether and how to enable authorization to the UE is FFS.

- Radio resource management for UE Reader operation:

- If the gNB has received the indication that a UE is authorized to operate as a UE Reader, then the gNB may assign radio resources to the UE for UE Reader operation.

- The UE Reader is assumed to request radio resources for Reader operation (e.g. taking into account assistance information received from the AIoTF) from the gNB.

NOTE 1: Assistance information is further clarified in other clauses.

NOTE 2: The details of UE Reader radio resource management will be defined by RAN WG2.

#### 8.1.3.2 User-plane option

The following additional principles apply:

- As depicted in Figure 8.1.3.2-1, the UE Reader connects to the AIoTF based on the AIoT Application Protocol (AIoT-AP) using an IP PDU Session between the UE and the UPF as transport. The related protocol stack is shown in Figure 8.1.3.2-2. The AIoT AP protocol will support procedures and information to be exchanged as specified by RAN WG2, RAN WG3 and SA WG2.



Figure 8.1.3.2-1: User-plane architecture for Topology 2



Figure 8.1.3.2-2: Protocol stack for the user-plane architecture for Topology 2

NOTE 1: Which transport protocol to use for AIoT-AP can be decided by CT WG1.

NOTE 2: Security for AIoT-AP is assumed to be defined by SA WG3.

- To operate as a UE Reader, the UE establishes a PDU Session to a specific DNN/S-NSSAI and establishes an association with the AIoTF identified by an FQDN using the AIoT AP protocol. In this release, the UE is preconfigured with the specific DNN/S-NSSAI and the AIoTF FQDN.

Editor’s note: Whether and which additional methods to dynamically provision the UE with this information can be specified and in which release is FFS.

- If the AIoTF determines that the UE is not authorized to operate as a UE Reader according to the UE’s subscription, then the AIoTF rejects the UE’s association request.

- If the AIoTF detects that the Reader function in the UE does not respond to a request by the AIoTF (e.g. an Inventory Request or Command Request), then the AIoTF considers the UE Reader unreachable and locally deletes the association for the UE Reader.

#### 8.1.3.3 RRC option

The following principles apply:

- Messages between the UE Reader and the AIoTF are delivered using RRC between UE and RRC and NGAP between gNB and AMF, and using an SBI interface between AMF and AIoTF. The related protocol stack is shown in Figure 8.1.3.3-1.

Editor's note: How addressing works for UL for Option B is FFS.

Editor's note: Further details how the RRC option works are FFS.



Figure 8.1.3.3-1: Protocol Stack for the RRC option

#### 8.1.3.4 Interim Conclusion for authorization

The following interim conclusion are agreed for the UE Reader authorization in Topology 2:

- The subscription data of UE Reader includes the indication that whether the UE is allowed to act as an AIoT Reader.

- The AMF provides the UE Reader authorization indication to the NG-RAN serving the UE Reader.

Editor's note: How to authorize the UE Reader will be determined later.

## 8.2 Conclusion on Key Issue #2

### 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.

Editor's note: The length of Identifier is fixed or dynamical is FFS.

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

Editor's note: Whether the temporary ID in the AIoT NAS layer is required for the privacy protection is FFS and is pending SA WG3 decision.

### 8.2.2 Subscription Management

The AIoT device may or may not have operator’s subscription data in the network. If the AIoT device doesn’t have the operator’s subscription data in the network, the corresponding related data (e.g. Device ID or credentials) is stored in the AAA server external to the network.

Subscription data for an Ambient IoT Device is required in case the Ambient IoT Device is managed by the network:

- It is used by the AIOTF to check whether the device is subscribed.

NOTE 1: Checking whether the device is subscribed needs coordination with SA WG3 study outcomes on validation of the ambient IoT Device identifier.

- It is dedicated subscription data for Ambient IoT Devices, i.e. different with UE subscription data.

- It contains at least a permanent Ambient IoT Device ID, etc.

NOTE 2: SA WG2 will align security related materials in subscription data with SA WG3 during the normative phase.

The Ambient IoT Device ID is used by the AIOTF together with local configuration, 3rd party related context to locate where the Subscription data or related data of an Ambient IoT Device is.

Editor’s note: Where to store the AIoT device subscription is FFS.

Subscription data for 3rd party AF is required:

- It is used by the AIOTF together with SLA and operator policy at NEF to perform authorization of the AF request targeting for Ambient IoT service. This includes: 1) checking whether the AF is authorized for the requested service operation; 2) checking whether the AF is authorized for the requested target area; 3) checking whether the AF is authorized for the requested target AIoT device(s).

- it is stored at UDM within 5G network.

NOTE 3: Items within the subscription data for 3rd party AF will be determined during normative phase.

UE Subscription data is enhanced to include an indication that whether the UE is allowed to operate as a UE reader.

## 8.3 Conclusion on Key Issue #3

### 8.3.1 General

The clause concludes the following aspects:

- Study how to support information transfer for Ambient IoT services and related system functionality, including the information transfer for an Ambient IoT device and for a group of Ambient IoT Devices.

NOTE: The above aspect includes studying whether there is a need to support session based transfer between Ambient IoT Device and the network considering the device types and capabilities.

- Study which of the enabled Ambient IoT services are exposed to AF and how, e.g. for the case AF requests Ambient IoT service for an Ambient IoT Device and for a group of Ambient IoT Devices.

### 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 or temporarily disabled.

- Enable: request to enable a temporarily disabled AIoT Device.

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

Editor's note: It is FFS whether and how to support enabling temporarily disabled AIoT devices.

### 8.3.3 NEF exposure

NEF supports to expose Ambient IoT service towards the AF.

- New NEF services (e.g. Nnef\_AIoT) to support the AIoT services including Service Operations of Inventory, Read, Write, and Permanent Disable will be defined.

### 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 to identify the target AIoT Device(s), target Readers and service operation specific parameters.

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 providing information to identify readers to include in the initial reader selection network. The information can identify multiple or an individual Reader to use for the request.

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 A-IoT 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 A-IoT Device Identification information with their own AIoT Device Identifier (part of or full AIoT Device Identifier) to determine whether respond to the paging message.

Editor's note: Whether and how the A-IoT Device Identification information will be security protected will be concluded by SA WG3.

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.

Editor’s note: If the “command-only” case applies, pending SA WG3, if a command and paging can be performed in a single operation, then an AIoT specific NAS message may be included in the request.

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, a TASK ID etc. 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.

### 8.3.5 Information provided by the AF

The AF provides one or some of the following information:

- Information about AIoT services:

- Service type indicating e.g. inventory or command (e.g. read or write).

- Information to be used for AIoT reader selection:

- At least one of the UE reader ID or the target area information.

- Optionally, Information about the target AIoT device(s):

- At least one of the AIoT device ID(s) or the filtering information which can be used to associate with multiple AIoT devices.

- Optionally, Information to be used for resource allocation that is detailed in TR 38.769 [8]:

- Approximate number of AIoT devices.

- Approximate D2R message size.

NOTE: Information to be used for resource allocation will be aligned with RAN WGs during the normative phase.

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