|  |  |
| --- | --- |
| 3GPP TR 23.700-13 V0.2.0 (2024-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Architecture support of  Ambient power-enabled Internet of Things  (Release 19) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms and abbreviations 7

3.1 Terms 7

3.2 Abbreviations 8

4 Architectural Assumptions and Requirements 8

4.1 Architectural Assumptions 8

4.2 Architectural Requirements 9

5 Key Issues 9

5.1 Key Issue #1: Architecture support of Ambient IoT Devices 9

5.1.1 Description 9

5.2 Key Issue #2: Identification, Subscription, Registration and Connection management 9

5.2.1 Description 9

5.3 Key Issue #3: Support of Ambient IoT Services 10

5.3.1 Description 10

6 Solutions 10

6.0 Mapping of Solutions to Key Issues 10

6.1 Solution #1: AIoT Temporary Identifier Control 10

6.1.1 Description 10

6.1.2 Procedures 11

6.1.3 Impacts on services, entities and interfaces 11

6.2 Solution #2: AIoT Device ID with home network, owner and instance identification 11

6.2.1 Description 11

6.2.2 Procedures 13

6.2.3 Impacts on services, entities and interfaces 13

6.3 Solution #3: Lightweight Ambient IoT system 13

6.3.1 Description 13

6.3.1.1 Introduction 13

6.3.1.2 Definitions 13

6.3.1.3 Assumptions 14

6.3.1.4 Reference architecture 14

6.3.1.5 Network function description 15

6.3.1.5.1 Reader 15

6.3.1.5.2 AIoT Controller 15

6.3.1.5.3 AF 15

6.3.1.6 Protocol Stacks 16

6.3.1.6.1 Protocol Stack between Reader and AIoT Controller 16

6.3.1.6.2 Protocol Stack between AIoT Device and Application Function 17

6.3.2 Procedures 18

6.3.2.1 Inventory procedure 18

6.3.2.2 Command procedure 19

6.3.3 Impacts on services, entities and interfaces 20

6.4 Solution #4: Simplified system for AIoT 20

6.4.1 Description 20

6.4.1.1 General 20

6.4.1.2 Abbreviations 21

6.4.1.3 Terms 21

6.4.1.4 Reference Architecture and NFs 21

6.4.1.5 Protocol Stack 23

6.4.2 Procedures 24

6.4.2.1 Inventory procedure 24

6.4.2.2 Command procedure 25

6.4.3 Impacts on services, entities and interfaces 26

6.5 Solution #5: NAS-based information transfer for Ambient IoT Services 26

6.5.1 Description 26

6.5.2 Procedures 26

6.5.3 Impacts on services, entities and interfaces 27

6.6 Solution #6: AIoT device authentication, ID validation and AIoT communication 27

6.6.1 Key Issue mapping 27

6.6.2 Functional Description 28

6.6.3 Procedures 29

6.6.4 Impacts on existing services, entities and interfaces 32

6.7 Solution #7: Bulk Introduction of Devices to the Network 32

6.7.1 Description 32

6.7.2 Procedures 32

6.7.3 Impacts on services, entities and interfaces 33

6.8 Solution #8: Inventory for AIoT Devices using AIOTF 34

6.8.1 Description 34

6.8.2 Procedures 36

6.8.2.1 Application Inventory Procedure 36

6.8.2.2 Periodic Inventory Procedure 39

6.8.3 Impacts on services, entities and interfaces 40

6.9 Solution #9: Information Transfer without a PDU Session 40

6.9.1 Description 40

6.9.2 Procedures 41

6.9.3 Impacts on services, entities and interfaces 42

6.10 Solution #10: Registration procedure for Ambient IoT Devices 43

6.10.1 Description 43

6.10.2 Procedures 43

6.10.2.1 Procedures for AF triggered Registration 43

6.10.2.2 Procedures for UE triggered Registration 45

6.10.3 Impacts on services, entities and interfaces 45

6.11 Solution #11: 5GC support for AF to retrieve data from AIoT devices 46

6.12 Solution #12: UE Function Delegation in Intermediate Node for AIoT Device 48

6.12.1 Description 48

6.12.2 Procedures 50

6.12.2.1 UFDM instantiation and provisioning 50

6.12.2.2 UFDM Registration 51

6.12.3 Impacts on services, entities and interfaces 52

6.X Solution #X: <Solution Title> 52

6.X.1 Description 52

6.X.2 Procedures 52

6.X.3 Impacts on services, entities and interfaces 52

7 Overall Evaluation 52

8 Conclusions 52

Annex <X> (informative): Change history 54

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the architecture support of Ambient IoT Devices, based on the services requirements defined in TS 22.369 [2] applicable to the Device types, traffic types, use cases and connectivity topologies defined in TR 38.769 [8].

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.369: "Service requirements for Ambient power-enabled IoT".

[3] 3GPP RP-234058: "New SID: Study on solutions for Ambient IoT (Internet of Things) in NR".

[4] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[6] 3GPP TS 23.503: "Policies and Charging control framework for the 5G System; Stage 2".

[7] 3GPP TR 38.848: "Technical Specification Group Radio Access Network; Study on Ambient IoT (Internet of Things) in RAN".

[8] 3GPP TR 38.769: "Study on solutions for Ambient IoT (Internet of Things) in NR".

[9] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[10] GS1 TDS Release 2.1: "EPC Tag Data Standard".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Ambient IoT Device:** An Ambient IoT device is an IoT device powered by energy harvesting, with limited energy storage capability. The other characteristics of the Ambient IoT device are defined in TR 38.769 [8].

NOTE 1: The final decision on the term name is to be determined in TR conclusion or normative phase.

**Ambient IoT Services:** The functionalities and procedures to support Ambient IoT use cases.

NOTE 2: the functionalities and procedures for Ambient IoT Services are left to outcome of the study. The Ambient IoT use case(s) can be referred to TR 38.848 [7] and TS 22.369 [2].

NOTE 3: The final definition on the term is to be determined in TR conclusion or normative phase.

**Device-originated - device-terminated triggered (DO-DTT):** The device originated traffic is triggered by the device terminated traffic or signalling.

**Device-terminated (DT):** The traffic is terminated at the AIoT device.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AIoT Ambient IoT

DO-A Device-originated - autonomous

DO-DTT Device-originated - device-terminated triggered

DT Device-terminated

# 4 Architectural Assumptions and Requirements

## 4.1 Architectural Assumptions

- The following traffic types for Ambient IoT Device are to be studied:

- DT: Device-terminated; and

- DO-DTT: Device-originated - device-terminated triggered.

NOTE 1: The DO-DTT additionally includes traffic from AIoT Devices, which is triggered by RAN/UE as reader, without CN sending traffic towards the AIoT Devices.

NOTE 2: The final decision for including DO-A (Device-originated - autonomous) in the study depends on RAN decision.

- The following two connectivity topologies as defined in TR 38.848 [7] are to be studied:

- Topology 1: BS <--> Ambient IoT Device;

- Topology 2: BS <--> intermediate node <--> Ambient IoT Device: Only a UE can act as an intermediate node which is under the network control.

- The communication spectrum is assumed to be licensed.

- Handover is not supported.

- RRC states are not supported by AIoT Devices (see TR 38.769 [8])

- No mobility (i.e. at least no cell selection/re-selection-like function) supported by AIoT Devices (see TR 38.769 [8])

Editor's note: The meaning of no mobility is to be clarified by RAN in TR 38.769 [8].

NOTE 3: Coordination with RAN is required to determine the Ambient IoT Device capabilities in relation to system level of functionality (considering e.g. traffic scenarios, connectivity topologies etc.).

NOTE 4: The security aspects for Ambient IoT requires coordination with SA WG3.

NOTE 5: The charging aspects for Ambient IoT will be studied by SA WG5.

NOTE 6: The NAS based Congestion control is not in the scope of this study.

## 4.2 Architectural Requirements

The following architectural requirements are applicable to this study:

- Support for AIoT Services needs to adhere to the nature of the AIoT Devices (e.g. ultra-low complexity, power, cost and resource-constrained).

- Support of the security aspects needs to consider the nature of the AIoT Devices (e.g. ultra-low complexity power, cost and resource-constrained) while addressing e.g. confidentiality, integrity, etc.

# 5 Key Issues

## 5.1 Key Issue #1: Architecture support of Ambient IoT Devices

### 5.1.1 Description

This key issue will address the system architecture to support Ambient IoT Devices, especially on the following aspects:

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

- Authentication and authorization for the Ambient IoT Device;

- Validation of the Ambient IoT Device identifier;

NOTE 1: Format of the Ambient IoT Device identifier is addressed in KI#2.

- Whether and how to secure device operations and services for an Ambient IoT Device or a group of Ambient IoT Devices;

NOTE 2: This key issue will take into account the outcome of RAN study in TR 38.769 [8].

NOTE 3: The security aspects related to this key issue, including the enable/disable device operation, requires coordination with SA WG3.

## 5.2 Key Issue #2: Identification, Subscription, Registration and Connection management

### 5.2.1 Description

This Key Issue pertains to the authorization and management of Ambient IoT Devices to support Ambient IoT services.

Considering that Ambient IoT Devices are a new type of reduced capabilities devices, the existing subscription model may not be suitable. Specifically, there is the need to study the device identification method to support Ambient IoT devices which are under operator control.

Based on the above consideration, the aspects to be studied in this key issue include:

- Study whether subscription management, registration management and/or connection management are necessary for an Ambient IoT Device or a group of Ambient IoT Devices, and if so identify the necessary state machine(s), procedures and functionality considering the Ambient IoT Devices capability and characteristics.

- Study whether and how reachability and paging apply to Ambient IoT Device(s) considering the Ambient IoT devices capability and characteristics, and if so, what are the impacts.

- Study how to identify Ambient IoT Device or group of devices and how to format the identifier.

NOTE: NAS based Congestion control are not in the scope of this study.

## 5.3 Key Issue #3: Support of Ambient IoT Services

### 5.3.1 Description

This Key Issue pertains to the AIoT services. Considering that AIoT Devices are a new type of devices with reduced capabilities, the following need to be supported:

- Inventory.

- Command.

NOTE 1: Further detailing of the inventory and commands will be addressed by solutions.

The key issue will study 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 2: 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.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
|  | Key Issues | | |
| Solutions | Key Issue #1 | Key Issue #2 | Key Issue #3 |
| #1 |  | X |  |
| #2 |  | X |  |
| #3 | X | X | X |
| #4 | X | X | X |
| #5 |  | X | X |
| #6 | X | X | X |
| #7 | X | X |  |
| #8 | X | X |  |
| #9 | X | X | X |
| #10 | X | X |  |
| #11 |  |  | X |
| #12 | X | X | X |

## 6.1 Solution #1: AIoT Temporary Identifier Control

### 6.1.1 Description

This solution addresses KI#2. The basic principle in 5GS is that the permanent subscriber identifier shall never be sent in clear text over Uu interface and a UE temporary identifier shall only be sent over Uu interface in clear text once e.g. when the UE is paged. This solution propose that same principle shall apply also for Ambient IoT.

The solution is based on the following assumptions:

- The AIoT device has higher complexity than a RFID tag that only reflects a preconfigured device ID when exited by RF power, but significantly lower complexity than a 3GPP CIoT device.

- The AIoT device has a non-volatile storage capability.

- The Temp ID generation algorithm is light weight but enough to avoid unauthorized AIoT device tracking.

### 6.1.2 Procedures

As the available power in an AIoT device is very limited, the message exchange between the device and the network must be minimized. The solution is based on the following principle:

* The initial temporary identifier (TempID) is known by both the CN NF and the AIoT device. After the AIoT device has been onboarded to the network the CN NF provision the AIoT device with the initial TempID and/or parameters to derive the initial Temp ID i.e.,. parameters for the Temp ID generation algorithm.

NOTE 1: Onboarding procedure will be studied under KI#2 and related conclusions needs to be considered when concluding the AIoT device Identifier control. It is assumed that during the onboarding procedure the CN NF can retrieve information from another NF or AF to onboard the AIoT device. The inital message from the UE during onboarding could e.g. include a URL or FQDN to establishing IP connection to a AF that holds additional onboarding information needed.

* Every time the TempID has been sent over the radio interface and a response from the AIoT device is sent, both CN NF and AIoT device locally generate a new TempID.

Editor’s Note: Details on the algorithm that locally generates a new TempID needs to be defined by SA3.

* In case the CN NF and the AIoT device TempID out of sync is detected, the CN NF and the AIoT re-synchronize the TempID.

Editor’s Note: How the out-of-sync detection and re-synchronization are performed is FFS, e.g. it may be a counter value not matching the expected value. Details depends on the Temp ID generation algortim.

* AIoT device considers and responds to the DT message if the AIoT device can match the TempID used in the DT message.
* AIoT device responds with DO-DTT message if the AIoT device can match the TempID used in the trigger message.

NOTE 2: The CN NF that manages the TempID will be defined together with the system architecture design to support the Ambient IoT in 5GC.

### 6.1.3 Impacts on services, entities and interfaces

Impacts on existing entities:

CN NF:

* Support the AIoT TempID handling including the generation of initial TempID, new TempID and re-synchronization between AIoT device and CN NF.

AIoT device:

* Recieving a initial TempID from the network.
* Generation of new TempID locally, when TempID used over Uu interface.
* re-synchronization between AIoT device and CN NF.

## 6.2 Solution #2: AIoT Device ID with home network, owner and instance identification

### 6.2.1 Description

This solution addresses the KI#2 and the aspect about how to identify and format the identifier of Ambient IoT Device in order to identify specific Ambient IoT Device or a group of Ambient IoT Devices.

In this solution, it is assumed that the Ambient IoT Device is configured with 3GPP-defined identifier and optionally be configured with 3rd Party-defined identifier in some specific scenarios.

According to TS 22.369 [2], the 5G system shall provide suitable mechanisms to support communication between an authorized 3rd party and an Ambient IoT device or group of Ambient devices. In addition, subject to user consent, operator’s policy and 3rd party request, the 5G system shall provide information about an Ambient IoT device or a group of Ambient IoT devices (e.g. position) to the 3rd party via the 5G network. Based on these service requirements, the relationship among the Ambient IoT Device, Mobile Network Operator and the 3rd party is illustrated below.



Figure 6.2.1-1: Relationship Among Ambient IoT Device, Mobile Network Operator and 3rd Party

It is assumed an Ambient IoT Device is owned by a third party who has a service agreement with a Mobile Network Operator to enable Ambient IoT service in 3GPP system. The MNO manages the Ambient IoT Device (e.g. holds the credentials of Ambient IoT Device, etc) in order to support communication between the 3rd party and the Ambient IoT Device via the 5G network. Therefore, based on this model, in the 3GPP system, different MNOs may need to manage different Ambient IoT Devices owned by different third parties. If uniqueness of Device ID cannot be guaranteed, operation of Ambient IoT services provided by 3GPP system may be impacted. Hence, considering of this, the Device ID used by an Ambient IoT Device shall enable the identification of the MNO it is managed by, the identification of the 3rd party it belongs and the identification of the Ambient IoT itself.

Based on the above consideration, following components are considered necessary to compose the Ambient IoT Device ID, which is defined by 3GPP:

- **Home Network Identifier:** an identifier used to identify the home MNO;

- **Owner Identifier:** an identifier used to identify a 3rd party who sends service requests to trigger 5GC to perform Ambient IoT service operation;

NOTE 1: The Owner Identifier is allocated by the home MNO corresponding to the Home Network Identifier.

Editor’s Note: The use of the Owner Identifier is FFS and may depend on the solution for Inventory, etc.

- **Instance Identifier:** an identifier used to identify a specific Ambient IoT device owned by the 3rd party.

NOTE 2: The Instance Identifier is allocated by the home MNO which may coordinate with the 3rd party.



Figure 6.2.1-2: Structure of Ambient IoT Device ID and optional 3rd Party-defined Identifier

The device can be configured with either:

- Only the 3GPP-defined identifier (i.e. Ambient IoT Device ID); or

- 3GPP-defined identifier (i.e. Ambient IoT Device ID) and 3rd Party-defined identifier.

The Ambient IoT Device ID is a permanent identifier used by the MNO to derive subscription-like data related to Ambient IoT Devices. In terms of each component of the Ambient IoT Device ID, the Owner Identifier has to be unique within the MNO identified by the Home Network Identifier. The Instance Identifier has to be unique within the Owner Identifier (which in turn is unique within a Home Network Identifier). The means that the Ambient IoT Device ID is unique globally. In this way, the length of the Ambient IoT Device ID can be shortened.

In the case of only a 3GPP-defined identifier, the 3rd party relies on the Ambient IoT Device ID allocated by the operator to perform Ambient IoT services.

Additionally, an Ambient IoT Device may be assigned an 3rd party-controlled identifier which, for example, can be used by the 3rd party to group Ambient IoT Devices together. As this identifier will not be used by the 3GPP system to uniquely identify the Ambient IoT Device, its allocation can be fully under the 3rd party’s control and the MNO can retain control of the allocation and management of the Device ID used to locate the subscription-like data for an Ambient IoT Device.

The 3rd party can use the 3rd Party-defined identifier component to perform Ambient IoT services on specific Ambient IoT devices.

For example, when a 3rd party (e.g. AF) sends a service request (e.g. inventory or command) to 5GC, the 5GC can trigger the reader(s) to inventory a group of Ambient IoT Device by broadcasting a partial/full Ambient IoT Device ID or partial/full 3rd Party-defined Identifier or both. The Ambient IoT Devices matching the broadcasted message will perform random access responding to the broadcast message. For example, when the partial value is the Home Network Identifier, Owner Identifier, the Ambient IoT Devices matching that the partial value (i.e. belonging to a specific 3rd party), or if the partial value is (part of) the 3rd Party-defined Identifier (i.e. matching the 3rd-party defined identifier), will respond to the broadcast message to perform random access and report their Device ID to the network.

With such format, the network can enable different group of Ambient IoT Device to respond the broadcast message for inventory.

Editor’s Note: It is FFS whether it can be assumed that the device and the CN can be pre-provisioned with Ambient IoT Device ID and the optional 3rd Party-defined identifier.

### 6.2.2 Procedures

How to utilize such format of Ambient IoT Device ID when network performs service operations will be specified in the call flows in other solutions.

### 6.2.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing services, entities and interfaces.

## 6.3 Solution #3: Lightweight Ambient IoT system

### 6.3.1 Description

#### 6.3.1.1 Introduction

This solution proposes a lightweight Ambient IoT system.

#### 6.3.1.2 Definitions

- **Command:** Refers to an instruction sent by an AF to an AIoT Device. The following instructions may be supported:

- Read: Reading data from an AIoT Device;

- Write: Writing data to an AIoT Device;

- Disable: Disable an AIoT Device temporarily or permanently.

- **Command Response:** Refers to the message sent by an AIoT Device in response to a Command. This may include an acknowledgement and optionally data (e.g., in case of the Read operation).

- **Enrichment Data**: Additional information that a Reader may include when providing Inventory information or a Command Response to the AIoT Controller. Enrichment Data may include information about the signal strength for each detected Device ID and the location of the Reader (if known).

- **Filter Criteria**: Criteria to limit an Inventory or Command to AIoT Devices that match certain criteria.

Editor's note: The details of Filter Criteria are FFS.

- **Inventory:** Refers to determining the identity of all or a subset of AIoT Devices in range of a reader.

#### 6.3.1.3 Assumptions

This solution makes the following assumptions:

- Commands and Command Responses are end-to-end protected between AF and AIoT Device.

NOTE 1: Details of the end-to-end protection of Commands and Command Results are assumed to be addressed by SA3.

- Commands and Command Responses are transparent to the AIoT Controller and the Reader, i.e., the AIoT Controller and Reader are not aware of the contents of Commands and Command Responses.

- AIoT Devices are assumed to be pre-provisioned with a Device ID and the security material for the end-to-end protection of Commands and Command Results.

Editor's note: Further details of the Device ID are FFS.

NOTE 2: Whether also dynamic (re-)provisioning of Ambient IoT Devices can be supported is up to SA3.

- The radio configuration (frequency bands, etc.) of the Reader is assumed to be configured through an OAM system, which is beyond the scope of SA2.

#### 6.3.1.4 Reference architecture

This solution proposes the reference architecture depicted in Figure 6.3.1.4-1.



Figure 6.3.1.4-1: Ambient IoT system architecture

The Ambient IoT system according to Figure 6.3.1.4-1 can support different deployment options. For example, the Reader may be co-located with a 3GPP UE so that the communication between Reader and AIoT Controller uses a PDU Session. Alternatively, Readers may be deployed independent of 3GPP UEs, i.e., as stand-alone base stations.

NOTE: The AIoT controller is assumed to be a 3GPP core network entity that enables Ambient IoT scenarios in the context of 5G. Other 5GC network functions are not assumed to be needed.

Editor's note: Whether NEF can potentially be reused for exposure (e.g., AF authorization, etc.) to the AF is FFS.

Editor's note: Further details how the architecture enables topology 1 and 2 are FFS. In case of topology 2, whether AMF is needed in 5GS core network is FFS.

#### 6.3.1.5 Network function description

##### 6.3.1.5.1 Reader

The Reader supports the following functionality:

- Supports the A-Uu air interface towards Ambient IoT Devices

- Registers with an AIoT Controller

- Supports the following functionality based on requests from an AIoT Controller

- Perform one-time or periodic Inventory, deliver Inventory result to AIoT Controller

- Delivers Commands from an AIoT controller to an AIoT Device

- Delivers Command Responses received from an AIoT Device to an AIoT Controller

##### 6.3.1.5.2 AIoT Controller

The AIoT Controller supports the following functionality:

- Register Readers

- Authenticate and authorize AFs

- Based on requests from an AF:

- Verify whether an AF is entitled to issue a specific Inventory Request

- Select Readers to fulfil Inventory or Command request by AFs

- Forward Inventory request to Readers and deliver Inventory result to AF

- Forward Command to Readers and Command Responses to AF

- Optionally collect usage data per AF, e.g., for charging purposes

- Store last known Reader information for AIoT Devices

Editor's note: Further details of exposure and charging are FFS.

##### 6.3.1.5.3 AF

The AF is assumed to support the following functionality:

- Authenticate towards the AIoT Controller

- Send Inventory and Command Requests

- Receive Inventory Responses and Command Responses

Editor's note: It is FFS how AF can discover the responsible AIoT controller.

#### 6.3.1.6 Protocol Stacks

##### 6.3.1.6.1 Protocol Stack between Reader and AIoT Controller



**Legend:**

- **Reader Application Protocol (R-AP):** Application Layer Protocol between the Reader and the AIoT Controller.

- **Service-based Interface (SBI) Protocol Stack:** The protocol stack for service-based interfaces as defined in TS 29.500 [9].

Figure 6.3.1.6.1-1: Control Plane between Reader and AIoT Controller

NOTE 1: Whether an SBI protocol stack (consisting of IP/TCP/HTTP2/JSON) as defined in TS 29.500 [9] or an SCTP-based stack will be used will be decided in coordination with RAN3.

NOTE 2: The R-AP protocol is assumed to be defined by RAN3 in coordination with SA2.

NOTE 3: The motivation to propose the R-AP protocol instead of reusing NGAP is that (a) NGAP terminates on the AMF, while AMF is not assumed to be used by this solution and (b) that most of the underlying concepts of NGAP (existence of UE contexts at RAN nodes, PDU Sessions, support of UE mobility, etc.) do not apply to AIoT in this solution.

Editor's note: Whether instead of a new R-AP protocol a simplified version of NGAP can be defined to support AIoT scenarios is FFS and can be discussed with RAN3.

Editor's note: Further details of using an SBI protocol stack-based interface between a Reader function co-located with a UE and the AIoT Controller over the PDU Session are FFS.

##### 6.3.1.6.2 Protocol Stack between AIoT Device and Application Function



**Legend:**

- **Reader Application Protocol (R-AP):** Application Layer Protocol between the Reader and the AIoT Controller.

- **Service-based Interface (SBI) Protocol Stack:** The protocol for service-based interfaces as defined in TS 29.500 [9].

- **AIoT API:** The API between AIoT Controller and Application Function to support Inventory and Command Procedures.

- **Command Protocol:** Application Layer Protocol between AIoT Device and Application Function to support Commands and Command Responses.

NOTE 1: The AIoT API is assumed to be defined by SA2 (Stage 2 aspects) and CT3 (Stage 3 aspects).

NOTE 2: The Command Protocol is assumed to be defined by SA2 (Stage 2 aspects) and CT1 (Stage 3 aspects).

### 6.3.2 Procedures

#### 6.3.2.1 Inventory procedure



Figure 6.3.2.1: Inventory procedure

1. The AF sends an Inventory Request to the AIoT controller. The AF may optionally include the following information:

- Filter Criteria to limit the inventory to AIoT Devices matching those criteria;

- a list of reader IDs to limit the inventory to specific Readers;

- a periodicity value to request the inventory to be performed periodically.

2. The AIoT controller verifies whether the AF is entitled to make the received Inventory Request, e.g., the AIoT controller verifies whether the AF is allowed to issue an Inventory Request with the specified Filter Criteria or without any Filter Criteria, without providing reader IDs, etc.

3. The AIoT controller sends the Inventory Request to the Readers identified by the Reader IDs or to all readers, includes the Filter Criteria and periodicity information, if provided by the AF.

4. Each Reader that received the Inventory Request from the AIoT Controller performs the Inventory procedure according to the Filter Criteria, if provided. The Readers either perform a one-time inventory or perform the inventory periodically according to the received periodicity.

5. One or multiple AIoT Devices respond to the Reader and provide their Device ID.

Editor's note: The details of how the Filter Criteria are applied during the Inventory procedure, e.g., to limit the AIoT device identities that are reported to an AF, are FFS.

6. The Readers collects the received Device IDs and provides the Device IDs to the AIoT Controller. The Readers may optionally include Enrichment Data.

7. For each reported Device ID, the AIoT Controller stores the reader ID that reported the Device ID together with a timestamp. The timestamp enables the AIoT controller to purge outdated last known Reader information; the details of this are up to AIoT Controller implementation.

8. The AIoT Controller provides the Device IDs and optionally the Enrichment Data to the AF.

Editor's note: Whether the AIoT Controller additionally provides the Reader ID for each Device ID (i.e., the last known Reader ID for each Device ID) to the AF is FFS.

#### 6.3.2.2 Command procedure



Figure 6.3.2.2: Command procedure

1. The AF issues a Send Command request, which includes the Command to be sent and either:

- a list of Device IDs that the Command is destined to, or;

- Filter Criteria that identify the AIoT Devices that are supposed to act upon the Command.

In addition, if the AF provides Filter Criteria, the AF may additionally include a list of reader IDs to use for sending the Command.

NOTE: Including the list of reader IDs enables the AF to limit sending of the Command to a specific area.

2. The AIoT Controller determines the list of Readers to use for sending the Command taking the Reader IDs (if provided by the AF) and any stored information about the last known Reader for specific Device IDs into account. The details of determining candidate Readers are up to AIoT Controller implementation.

3. The AIoT Controller provides the Command and the Device IDs or Filter Criteria (whichever has been provided by the AF) to the Readers.

Editor's note: Whether the Reader needs to perform an Inventory before sending the command to the AIoT devices is FFS.

4. Each Reader that receives the Send Command request from the AIoT Controller, sends the Command to the AIoT Devices identified by the Device IDs or to the AIoT Devices identified by the Filter Criteria (whichever has been provided by the AIoT Controller).

Editor's note: The details of how the Filter Criteria are applied during the Command procedure are FFS.

Editor's note: Failure handling, e.g., if an AIoT device is not reachable is FFS.

5. The AIoT Device(s) respond to the Reader and provide the Command Response.

6. The Readers send the received Command Response(s) to the AIoT Controller. The Readers may optionally include Enrichment Data.

7. The AIoT Controller sends the received Command Response(s) and optionally Enrichment Data to the AF.

NOTE: Support of sending the same Command to multiple AIoT Devices requires support of group security for the Command (e.g., group keys for protecting the Command), which depends on SA3.

### 6.3.3 Impacts on services, entities and interfaces

New network entities and interfaces are proposed.

## 6.4 Solution #4: Simplified system for AIoT

### 6.4.1 Description

#### 6.4.1.1 General

The solution addresses KI#1, #2 and KI#3.

It provides an e2e solution to support AIoT services with regard to topology1 and 2.



Figure 6.4.1.1-1: Topology 1&2

The following assumptions are taken into account for the solutions

- No matter what Topologies are applied (including more topologies in future release), The Topologies types are transparent to the AIoT devices and the AIoT devices are common designed.

- In topology2, when the UE out of Uu coverage in some blind area but the AIoT air coverage goes well, the AIoT operation at the UE reader will not stop and continue.

- The AIoT Air interface is assumed to be a new air interface and layers above the AS layer is in the scope of SA2 study.

#### 6.4.1.2 Abbreviations

#### 6.4.1.3 Terms

The following terms are used for the solution:

- **AIoT operation:** the operation with communicating to AIoT devices, e.g. inventory and command.

- **Inventory**: filter and/or discovery one or multiple Ambient IoT device(s).

- **Command**: e.g. read**,** write, control, enable or disable one or multiple Ambient IoT device(s).

- **AIoT function:** the NF providing management and control for AIoT services and AIoT operation.

- **AIoT API:** the service-based API to provide AIoT Services which can be invoked by the AF.

- **AIoT Air interface:** the air interface between reader and AIoT devices.

- **Reader:** the device which supports to communicate one or multiple Ambient IoT device(s). It can operate as a UE and be called UE reader, or can operate as a RAN node and be called RAN reader.

#### 6.4.1.4 Reference Architecture and NFs



Figure 6.4.1.4-1 the example of reference architecture which supporting topology1&2

Up to different deployment, the above NF may be collocated or standalone. The above reference architecture can be separate into the following alternatives:

- Alternative1: a standalone network supporting AIoT functionality only.

- Alternative2: a network supporting both legacy 5GS functionality and additional AIoT functionality.



Figure 6.4.1.4-2 the example of reference architecture for alternative1



Figure 6.4.1.4-3 the example of reference architecture for alternative2

The functionalities may include the following NFs and/or devices:

- The reader (i.e. UE reader and/or RAN reader).

NOTE: a 5GS UE may additionally support UE reader functionality. a NG RAN may additionally support RAN reader functionality.

- The AIoT Function: provides the AIoT control, which may be collocated with AMF or a standalone NF.

- In some scenario (e.g. operator owned AIoT devices), there might be ta UDM which stores the data of AIoT device.

Editor's note: It is FFS whether it can be assumed for all scenarios that the device and the CN can be pre-provisioned with CN level per device information (e.g. network layer AIoT device ID, security material).

- The NRF is responsible for NF discovery as legacy and support AIoT function discovery.

- The Authentication Function (e.g. AUSF/AAA) provide authentication for AIoT devices. The Authentication Function may be located in the serving network or in the 3rd party

- The NEF is responsible to authorize the AF request as legacy and support the new scenario of AIoT, i.e. authorize the AIoT operation request from the AF.

#### 6.4.1.5 Protocol Stack



Figure 6.4.1.5-1: protocol stack example for Topology1



Figure 6.4.1.5-2: protocol stack example for Topology2

Both the App layer and the AIoT layer are beyond the AIoT AS layer and belongs to non-access layer.

- The App layer are used to transmit the information between the AIoT device and the Server.

- The AIoT layer is used to transmit the information between the AIoT device and UE reader / CN.

### 6.4.2 Procedures

#### 6.4.2.1 Inventory procedure



Figure 6.4.2.1-1: Inventory Service Flow

1. AF sends Inventory Operation Request with the following information: target area for the operation, client which requests the operation, match information which is used to filter and discover the target AIoT devices for the operation.

2. The NEF authorizes the AF request. If the AF request is authorized, The NEF discovers the AIoT function using the information in Inventory Operation Request, e.g. using the target area for the operation to discovery the AIoT function from NRF. If the target area for the operation matches the AIoT service area of the AIoT Function, the NRF returns the information for the AIoT function to the NEF.

3. The NEF forwards the Inventory Operation information to each the selected AIoT function.

4. AIoT function discovers and selects reader (i.e. UE reader(s) and/or RAN reader(s)) to perform Inventory Operation according to the Inventory Operation information. e.g. using the target area for the operation to discovery the readers. If the target area for the operation matches the AIoT service area supported by the readers, those readers can be selected for execute the inventory operation.

Editor's note: It is FFS how to discover and select UE readers.

5. For each of the selected reader, the AIoT Function sends Inventory with the Inventory Operation information.

6. The select reader executes the inventory operation towards the target AIoT Devices.

7. The AIoT device which matches to the match information will responses the AIoT device information (e.g. the device ID) to the reader and the AIoT device authentication procedure may be triggered. The step7 can be repeated for multiple AIoT devices.

NOTE: How the AIoT device authentication performed is left to SA3.

8-9. AIoT Function report the successfully discovered AIoT device(s) to the AF vie NEF.

#### 6.4.2.2 Command procedure



Figure 6.4.2.2-1: Command Service Flow

1. AF sends a command request along with the following information: target area for the operation, client which requests the command operation, match information which is used to filter and discover the target AIoT devices for the operation container.

NOTE 1: The command procedure in this solution assumes the command content is transparent to the CN and can be carried by some container between the AIoT device and AF.

2. The NEF authorizes the AF request. If the AF request is authorized, The NEF discovers the AIoT function using the information in the Operation Request. How AIoT function is discovered and select is as described in step2 in clause 6.4.2.1.

3. The NEF forwards the Operation information to each the selected AIoT function.

4. AIoT function discovers and selects reader (i.e. UE reader(s) and/or RAN reader(s)) to perform the Operation according to the Operation information. How reader is discovered and selected is as described in step4 in clause 6.4.2.1.

5-7. Discover the target AIoT devices. How to discover and authenticate the AIoT devices is similar as that within the inventory operation procedure. The AIoT device may also authenticate the reader during the procedure.

NOTE 2: How the reader is authenticated by the AIoT device and how AIoT device is authenticated is left to SA3.

8-9. The reader sends the Operation container to each of the target AIoT devices.

10-11. AIoT Function report the operation result to the AF vie NEF/ASAF.

### 6.4.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing services, entities and interfaces.

## 6.5 Solution #5: NAS-based information transfer for Ambient IoT Services

### 6.5.1 Description

The solution applies to both the Key Issue #2 "Identification, Subscription, Registration and Connection management" and the Key Issue #3 "Support of Ambient IoT Services". This solution applies to Topology 1.

Considering the nature of the AIoT Devices (e.g. ultra-low complexity power, cost and resource-constrained), the PDU Session/QoS Flow based data transfer is not suitable for such AIoT Devices. This solution proposes to use NAS-based message for information transfer for Ambient IoT Services. The AF requests service operation for an AIoT Device or a group of AIoT Devices via the NEF, and the service operation is forwarded to the AMF/AIoTF (new function introduced to support AIoT services) which then triggers the N2 like procedure and AS procedure to the AIoT Devices. After receiving AS message, the AIoT Devices includes Device ID and AIoT data requested by service operation in the NAS message and send it to the AMF/AIoTF, and then the AMF/AIoTF sends the Device ID and AIoT data to the AF via the NEF.

### 6.5.2 Procedures

Depicted in Figure 6.5.2-1 is the procedure for NAS-based information transfer for Ambient IoT Services.



Figure 6.5.2-1: Procedure for NAS-based information transfer for Ambient IoT Services

1. AF sends a AIoT Service Request (AF Identifier, Device ID, service operation) message to the NEF. The service operation indicates the service (e.g. Inventory, Command) the AF requested for the Ambient IoT Device(s). Device ID is used to identify an Ambient IoT Device or a group of Ambient IoT Devices.

Editor's note: Whether service operation is an end-to-end parameter between AF and Ambient IoT Device is FFS.

2. The NEF checks if the AF is authorized to request the AIoT service.

3. The NEF selects the AMF/AIoTF supporting AIoT service and forwards the service operation to the AMF/AIoTF using AIoT Service Request (Device ID, service operation) message.

Editor's note: The details on AMF/AIoTF selection and Reader (BS) selection are FFS.

4. The AMF/AIoTF sends a N2 like message (NAS message (Device ID, service operation)) to Reader (BS).

Editor's note: Whether existing NAS message is reused or new NAS like message is defined is FFS.

5. The Reader (BS) performs AS procedure with Ambient IoT Devices. The NAS message (Device ID, service operation) is included in the AS message to Ambient IoT Devices.

6. For each Ambient IoT Device, if Ambient IoT Device receives AS message and is matched with the Device ID, the Ambient IoT Device initiates Random Access like procedure.

NOTE: The steps 5 and 6 are to be defined by RAN WGs.

7. The Ambient IoT Device sends NAS message (Device ID, AIoT data) over AS message. AIoT data is included in the NAS message if requested by the service operation.

8. The NAS message is forwarded by Reader (BS) to the AMF/AIoTF.

Editor's note: The security protection of NAS message is FFS.

9. The AMF/AIoTF checks if the Ambient IoT Device is authorized to transfer the AIoT data.

Editor's note: It is FFS whether it can be assumed for all scenarios that the device and the CN can be pre-provisioned with CN level per device information (e.g. network layer AIoT device ID, security material).

10. The AMF/AIoTF responds to the NEF using AIoT Service Response (Device ID, AIoT data) message.

11. The NEF responds to the AF using AIoT Service Response (Device ID, AIoT data) message.

### 6.5.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing services, entities and interfaces.

## 6.6 Solution #6: AIoT device authentication, ID validation and AIoT communication

### 6.6.1 Key Issue mapping

This solution addresses the following requirements:

- from Key Issue #1 the requirement:

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

*- Validation of the Ambient IoT Device identifier;*

*- Whether and how to secure device operations and services for an Ambient IoT Device or a group of Ambient IoT Devices;*

- from Key Issue #2 the requirements:

*- Study whether subscription management, registration management and/or connection management are necessary for an Ambient IoT Device or a group of Ambient IoT Devices, and if so identify the necessary state machine(s), procedures and functionality considering the Ambient IoT Devices capability and characteristics.*

*- Study whether and how reachability and paging apply to Ambient IoT Device(s) considering the Ambient IoT devices capability and characteristics, and if so, what are the impacts.*

- from Key Issue #3 the requirements:

*- 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: Including 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.*

### 6.6.2 Functional Description

The security protection of AIoT data can be categorized in the following way:

* Application layer security between the AIoT device and AIoT server. The application layer security is outside the scope of 3GPP.
* Network layer security between the AIoT device and network (NG-RAN and 5GC). The AIoT data/signalling transmitted to/from the AIoT devices may need to be security protected, i.e. encrypted and/or integrity protected.

This solution proposes to apply network layer security protection between the AIoT device and a new NF called Ambient AIoT gateway (AIoT-GW) which is introduced in the 5GC control plane. The AIoT-GW also handles the AIoT information transfer from the 5GC to the AIoT devices.

The assumed architecture for AIoT device authentication and communication is shown in Figure 6.6.2-1. The architecture covers both topology 1 and topology 2 as introduced in Architectural Assumptions in clause 4.1. The AIoT reader includes either a UE as intermediate node or base station (BS) node.

It is assumed that the AIoT reader and the AIoT-GW establish an association for AIoT communication as follows:

* The BS acting as AIoT reader establishes a N2’ association with the AIoT-GW where the protocol used on the N2’ association may be a different from NGAP or simplified NGAP.
* The UE acting as AIoT reader is registered with the AMF via the N1 interface. The communication between the UE and AIoT-GW is not in the scope of this solution, i.e. will be described in solutions for topology 2 (e.g. the UE may exchange with the AIoT-GW via a PDU Session or the AMF may register the UE with the AIoT-GW like registering with the SMSF, etc.).



**Figure 6.6.2-1: Assumed architecture for AIoT device authentication and AIoT communication**

In particular, this solution applies for inventory AIoT service or other services where the destination of the AIoT data/signalling is either a group of AIoT devices or all devices subscribed for the AIoT service The main principles of the solution are as follows:

- The security protection of the DL AIoT data/signalling is created in the AIoT-GW by applying either 1) the group/service credential(s) corresponding to the destination group/service ID or 2) the credentials corresponding to the destination individual AIoT device ID. The AIoT device uses the preconfigured credential(s) corresponding to the destination ID (i.e. either group ID or individual ID) to verify the received DL AIoT data/signalling.

- The security protection of the UL AIoT data/signalling is created in the AIoT device by applying individual credential corresponding to the individual device ID. The individual device ID is transmitted together with the UL AIoT data. The AIoT-GW uses the device individual credentials from the AIoT device subscription data to verify the device individual ID and the UL AIoT data/signalling.

It is further proposed that the AIoT devices do not implement USIM module, do not register with the 5GS and no CM state is maintained in the 5GS. The UDM/UDR is provisioned with AIoT device subscription data which may contain (in addition to the identifiers and credentials) a status and location for the device. The status and location of the AIoT device can be updated in the UDM by the AIoT-GW when the AIoT device sends AIoT data/signalling.

Editor’s Note: The storage of AIoT device subscription in the of UDM/UDR is intended for the use case of network-controlled authentication/verification of the AIoT device. This assumption of network-layer security for the AIoT device will be evaluated during the conclusion phase.

Editor’s Note: This solution assumes 1) the transmission of the IDs over the radio interface without encryption and 2) the use of group credentials for security protection (e.g. configured in the UDM/UDR and AIoT device). Coordination with the SA3 WG is needed to verify the feasibility.

### 6.6.3 Procedures

The Figure 6.6.3-1 describes the signalling flow for the authentication and ID validation of AIoT devices and secure AIoT communication.



**Figure 6.6.3.1-1: Signalling flow** **for the authentication and ID validation of AIoT devices and** **secure AIoT communication**

The detailed description of the steps is provided as follows:

0a. The AIoT device is (pre-)configured with a device individual identifier and corresponding credentials, as well as with group/service identifier and corresponding credentials.

- Device individual ID and corresponding credentials are used for the security protection of the individual ID and the AIoT data destined to the individual ID. The device ID may be in the format of <hardwareID@MNO-ID> or <hardwareID@manufacturer-ID>.

- Group (or service) ID and corresponding credentials are used for the security protection of the group ID and AIoT data destined to the group ID. The group/service IDs may be in the format of <applicaitonID@SP-ID> wherein the SP-ID is the service provide ID or AIoT AF/AS ID.

0b. The UDM/UDR is provisioned with subscription data for each AIoT device, for which the AIoT service is enabled in the communication system. The AIoT device subscription data can include the following parameters:

- Individual device ID and corresponding credentials for security protection;

- a list of AIoT services (or applications) for which the device is subscribed, including the group/service IDs and corresponding credentials for security protection.

- a status of the individual ID validation, e.g. the status being success or failure. This status may be updated by the AIoT-GW when the AIoT-GW performs verification of the individual device ID, e.g. when the AIoT device sends UL AIoT data.

- enabled or disabled state for the AIoT device. It means whether the AIoT device is allowed or not allowed to transmit AIoT data or to be on service.

- location information of the AIoT device, e.g. last AIoT reader node ID or AIoT cell ID.

1. The AIoT-GW is triggers DL data/signalling to the AIoT device. This may be triggered by data received from the AIoT AF/AS. The request from the AIoT AF/AS can include: AIoT Session ID, list of destination transmission areas, destination Group ID or list of Device IDs, AIoT data (e.g. containing a “command” to the device) which may include the AIoT service type, priority for the AIOT data transmission, reporting AIoT AS address.

2a. The AIoT-GW may retrieve from the UDM either the AIoT device subscription data (if device individual ID is included instep 1), or service/application subscription data or both.

2b. The response from the UDM may include the information described in step 0b.

3. The AIoT-GW stores the IoT data/signalling for DL transmission. In this sense, the AIoT -GW applies the store-and-forward functionality for DL data.

4. The AIoT-GW can send a response to the AIoT AF to acknowledge (or indicate failure) that the AIoT data/signalling from step 1 has been authorised and stored for DL transmission.

5. The AIoT-GW creates DL AIoT signalling for transmission or store the AIoT data received received in step 1. The AIoT signalling is meant to be processed by the AIoT reader node which performs the AIoT radio transmission. The DL AIoT data/signalling may contain:

- destination identifier, e.g. individual device ID or group ID.

- service/application identifier, e.g. AIoT service ID, which is meant to identify the AIoT application at the AIoT device, since there may be multiple AIoT applications installed or running at the AIoT device. This identifier may further include a port ID of the AIoT application.

- DL Message Authentication Code (MAuC) corresponding to the destination identifier,

- DL AIoT signalling or DL AIoT data. The difference is that the AIoT signalling is used for inventory type of service where no data/command is written in the AIoT device, whereas the AIoT data carries a data/command to be written or stored in the AIoT device.

- destination transmission area, priority, etc..

The AIoT-GW also selects an AIoT reader node (e.g. BS or UE as intermediate node) to which to forward the request for AIoT data/signalling transmission.

6. The AIoT-GW sends the AIoT data/signalling request message to the selected AIoT reader. The AIoT data request message may the parameters listed in step 5.

7. The AIoT reader transmits the received AIoT data or AIoT signalling over the radio interface to the AIoT device.

8a. The AIoT device verifies whether the authentication code (e.g. MAuC) and the destination identifier (device ID or group ID) are correct by using the credential as described in step 0a.

8b. The AIoT device creates an UL AIoT data/signalling for transmission (e.g. for backscattering). The UL message or PDU is transmitted using the individual device ID and security protected by UL MAuC created with the credentials corresponding to the individual device ID.

9. The AIoT reader can create and sends an AIoT report to the AIoT-GW. The AIoT report includes the device ID, UL MAuC, AIoT service ID, AIoT data/signalling, AIoT reader ID (e.g. including the location identifier).

10. The AIoT-GW verifies the Device ID and/or UL MAuC using the credentials for the individual device ID (e.g. received in step 2b).

11. The AIoT-GW creates and transmits a notification message to the AIoT AF/AS which includes AIoT Serving ID, AIoT signalling result (Device ID, status (e.g. type of good to which the device is attached), ID verification failed/succeeded), AIoT device location.

12. The AIoT-GW can update to the UDM for the AIoT device ID status (e.g. verified ID) or device location.

### 6.6.4 Impacts on existing services, entities and interfaces

The following NFs and interfaces are impacted:

- AIoT-GW: a new NF with the functionality described in clause 6.6.2.

- AIoT reader (BS or UE as intermediate node): supporting 1) AIoT capabilities to communication with the AIoT devices and 2) capabilities to receive and store AIoT signalling/data from the an AIoT-GW and to transmit AIoT report to the AIoT-GW.

- UDM/UDR: store AIoT device subscription data and AIoT application subscription data.

## 6.7 Solution #7: Bulk Introduction of Devices to the Network

### 6.7.1 Description

This solution is targeting KI#2 Identification, Subscription, Registration and Connection management. It is related with KI#1 as well.

Regarding the Registration, the following should be considered.

- AIoT Devices have ultra-low complexity/power/cost and are resource-constrained

- The network needs to support a huge number of AIoT Devices

Considering the above, registration from each of the AIoT Device to the network is difficult both for the AIoT Device and for the network.

This solution proposes a Bulk Introduction of Devices to the Network performed by AF based on pre-Registration of Ambient IoT Devices (Stores the credentials of Ambient IoTs per a service). The pre-Registration of Ambient IoT Devices may be done during provisioning phase, even before Ambient IoT Device deployment.

It is assumed that UDM is provisioned with the Ambient IoT Device data before bulk introduction procedure.

After this Bulk Introduction of Devices to the Network, AMF has context for the Ambient IoT devices, and so the messages from the devices need not undergo additional authentication/authorization checks.

### 6.7.2 Procedures

Bulk Introduction of Devices to the Network procedure for Ambient IoT ID is depicted in Figure 6.7.2-1.



Figure 6.7.2-1: Bulk Introduction of Devices to the Network procedure for Ambient IoT

0. Before deployment, Registration of Group of Ambient IoTs via AF is done. AF stores all the credentials of Ambient IoTs per a service

1. Bulk Introduction of Devices to the Network Request sent by AF to NEF. Bulk Introduction of Devices to the Network Request includes AF ID, list of device IDs, Registration Type. The Registration type can be Group Initial Registration.

2. Delivering the request information to the relevant AMF.

Editor’s note: How to find relevant AMF is FFS, For example, AMF can be selected by pre-configuration.

Editor’s note: In this step, whether and how the procedure for Authentication for Group of Ambient IoT devices is FFS.

3. NEF sends Bulk Introduction of Devices to the Network Accept to AF.

### 6.7.3 Impacts on services, entities and interfaces

AF:

- Performs Bulk Introduction of Devices to the Network with the PLMN. This Registration of devices can be done before deployment.

- Stores all the credentials of Ambient IoTs per a service

NEF:

- Supports signalling for Bulk Introduction of Devices to the Network between AF and AMF

AMF:

- Supports Bulk Introduction of Devices to the Network of Ambient IoT Devices

- Retrieves Access and Mobility Subscription data for group of devices from UDM. Subscription data for group of devices can be stored in AF.

- Creates UE context of group of devices. UE context of group of devices is identified by AF ID.

UDM:

- Supports retrieval of subscription data for group of devices from UDM

- May authenticate and authorize whole devices at a time

## 6.8 Solution #8: Inventory for AIoT Devices using AIOTF

### 6.8.1 Description

This solution addresses subscription, registration and connection management aspect of Key Issue #2, which is based on the following system architecture.

The functional entities defined in TS 23.501 [4] are reused with the exception for the following additions:

- Ambient IoT Function (AIOTF): AIOTF is introduced to support AIoT services, with some AMF’s functionalities integrated, which includes:

- A-RAN (Ambient IoT RAN) connectivity.

- Inventory handling and device context management.

- Authentication and authorization for the access, which triggers interaction with AUSF/UDM

- Collect charging data and interact with CHF for charging.

- Routing the request from AF (via NEF) to A-RAN, for DO-DTT/DT traffic types.

- Routing the response from A-RAN to AF (via NEF) for DO-DTT traffic type.

Editor's note: It is FFS whether AIOTF needs to support further functionalities.

- UDM: UDM is enhanced to store and manage the AIoT device information. The device information contains the device ID, device status information (e.g. enabled/disabled/permanently disabled), as well as CN related information (e.g. serving NF).

- NEF: NEF is enhanced to expose AIoT specific services towards AF.

- CHF: CHF is enhanced for the charging for AIoT services.

NOTE 1: The charging aspects is to be studied by SA5.

- NRF: NRF is enhanced to support the new NF type AIOTF and the corresponding NF profile.

- AUSF: AUSF is enhanced for the authentication for the access from AIoT devices.

NOTE 2: The security aspects are to be studied by SA3.

Editor's note: The functions of the NFs need to be updated to align with the solutions for KI#2 and KI#3, and to be aligned with A-RAN WGs, SA3 (for security), SA5 (for charging).

Editor's note: It is FFS whether it can be assumed for all scenarios that the device and the CN can be pre-provisioned with CN level per device information (e.g. network layer AIoT device ID, security material)

The Figure 6.8.1-1 illustrates the enhanced architecture to support AIoT devices using AIOTF for inventory.



Figure 6.8.1-1: System Architecture to support AIoT Devices using AIOTF for Inventory

Editor's note: It is FFS whether and how to address other services/use cases than inventory with this architecture.

Editor's note: It is FFS whether and how much of NGAP is re-used for interface between A-RAN and AIOTF.

This solution focuses on Topology 1.

Editor's note: It is FFS whether and how the solution can be evolved for Topology 2.

The AIoT device information can be stored in UDM, which is similar as the subscription data. The device information contains the device ID, device status information (e.g. enabled/disabled/permanently disabled), as well as CN related information (e.g. serving NF).

For enabling registration management, the some AIoT devices are assumed not to be able to initiate the registration on their own. However, such passive AIoT devices can respond to messages from the network, which make them discoverable by the network. The procedure that is used to make the AIoT devices discoverable can be called an inventory procedure.

Editor's note: It is FFS whether none of the AIoT device types can initiate registration on their own.

The inventory procedure can be triggered by an AF sending an inventory request towards CN, and CN sends a request to A-RAN. The AIoT devices respond to the inventory request from A-RAN and send their device IDs. Such inventory procedure triggered by an AF can be called application inventory procedure.

The AF may further provide the inventory strategy information (e.g., inventory frequency, inventory period) to enable CN or A-RAN to perform periodic inventory to allow the newly coming AIoT devices to be discovered, without further explicit requests from the AF.

For the application inventory or periodic inventory, depends on device capabilities, the authentication and authorization may be performed, and the CN allocated device ID which is similar as 5G-GUTI may be passed to the device. For those devices, the device contexts are stored in AIOTF, including the security contexts.

When application inventory or periodic inventory procedure is triggered, the network may indicate whether all targeted devices need to respond the inventory, or only those devices which haven’t been “inventoried” towards this A-RAN node should respond.

When AIoT devices move to a new A-RAN node, by responding the inventory, the network can also keep track of the AIoT devices location e.g. on a serving A-RAN node granularity, so that the network can route the request effectively which is sent from the AF to one or more specific AIoT devices.

NOTE 3: When AIoT devices move, the AIoT devices does not perform cell re-selection like logic.

For connection management, when in CM-CONNECTED state, the device is known by the network and DL data can be delivered to the service A-RAN node directly. When in CM-IDLE state, the detailed location of the device is unknown, so that before delivering DL data, CN needs to look up the device.

Editor's note: It is FFS whether there are needs to enable functionality enabling similar functionality as CM-IDLE and CM-CONNECTED states enables, and whether CN (i.e., AIOTF) needs to perform different actions accordingly, when DL data need to be delivered.

### 6.8.2 Procedures

NOTE: The message names in the procedures below are descriptive. It is assumed that the names are updated with corresponding SBI based names where applicable during the normative phase.

#### 6.8.2.1 Application Inventory Procedure

The application inventory procedure is initiated by the AF to discover one or more AIoT devices in a specific area.



Figure 6.8.2.1-1: Inventory Procedure

1. The AF sends Inventory Message Request to the NEF, containing the area information, device information, optional inventory strategy information, and optional report aggregation info.

- The area information could be the external geographical area information.

- The device information could be device ID, device group ID, and/or device type.

Editor's note: Details of device type is FFS.

- The inventory strategy information contains, e.g., the inventory frequency and inventory period to guide the readers to perform the inventory periodically. It also indicates whether all the targeted devices need to respond (full inventory), or only those who haven’t performed the inventory procedure (delta inventory) should respond.

- The location required indicates whether the AF requests the location information of the AIoT devices provided.

- The report aggregation info indicates whether the reports need to be aggregated or not for a specific aggregation period, and whether the reports are needed after the aggregation period.

2. The NEF authorizes the request from the AF and perform the area translation to translate external area information to the internal area information. Within the authorization, the NEF further check whether the AF is authorized to get the location information of the device.

3. The NEF sends NRF query with internal area information to query AIOTFs serving the area.

4. The NEF sends the Inventory Request to the AIOTFs with the internal area information, device information and optionally inventory strategy information, optional location required information.

5. The AIOTF discovers A-RANs based on internal area information.

6. The AIOTF sends an NGAP message (Inventory Request) to the A-RANs with the internal area information, device information and inventory strategy information, and optional location required information.

7. The A-RAN (reader) initiates inventory based on device information as well as the inventory strategy information provided by the AF. The A-RAN may provide reader identity information (e.g. A-RAN ID) to enable the AIoT devices to understand they are read by which A-RAN node.

8. The AIoT Device reports the device ID, and optional device capability information. If the Inventory procedure indicates only who haven’t performed the inventory procedure should respond, and if the AIoT Device has performed the inventory procedure towards this A-RAN node, it should skip the reporting.

9. The A-RAN sends an NGAP message (Inventory Response or Inventory Notify) to the AIOTF, containing the device ID and the optional device capability information provided by the device. The A-RAN may further provide location information (ULI) of the device, if requested from the AIOTF and allowed by local policy. The A-RAN may further provide an end indicator to inform the AIOTF whether it is the last inventory response for the inventory round.

Editor's note: Details of what location information A-RAN provides is FFS.

10. The AIOTF validates the device ID via interacting with AUSF and UDM. The AIOTF may further check the device capability information from the device subscription data stored in the UDM for the device capability information.

Editor's note: The check of the device capability information and device ID is FFS.

Editor's note: It is FFS which entity defines the AIoT device info and how to store such info in the UDM.

Based on the device capability info from the device and/or device information data in UDM, if the AIoT device is capable of handling authentication and authorization, step 11 – step 13 are executed:

Editor's note: The use of the step 11-13 is FFS.

11. The AIOTF together with AUSF and UDM, triggers authentication and authorization procedures towards the AIoT device.

12. The AIOTF may further allocates CN device ID and sends to the AIoT device.

13. The AIOTF registers with the UDM (UECM) for the device access.

14. The AIOTF may perform aggregation for the device ID, based on the report aggregation information provided by the AF. Within the aggregation period, the AIOTF will buffer the device IDs reported from the AIoT devices. The AIOTF may stop buffering and send report immediately, if it receives end indicator from A-RAN in step 9. When the aggregation period expires, the AIOTF sends the report. For those device ID report after the aggregation period, if it is needed by the AF, the AIOTF sends the report. Otherwise, it will be dropped.

15. The AIOTF sends Inventory Response or Notification Request towards the NEF for the device ID or the aggregated device ID information.

16. The NEF sends Inventory Response or Notification Request towards the AF for the device ID or the aggregated device ID information.

#### 6.8.2.2 Periodic Inventory Procedure

The periodic inventory procedure is initiated by the CN or A-RAN, which follows the instructions from the AF,



Figure 6.8.2.2-1: Periodic Inventory Procedure

The AIOTF or the A-RAN may initiate the periodic inventory procedure based on the inventory strategy information provided by the AF, to enable the AIoT devices to be discovered when they newly enter the coverage area.

0. An Inventory Procedure may have taken place resulted in inventory strategy information stored in the AIOTF. e.g. inventory frequency

The step 1 - step 11 are similar as step 6 - step 16 in clause 6.8.2.1, with the following additions:

1. It will be performed only when it is AIOTF to initiate the periodic inventory. The inventory strategy should be set to delta inventory.
2. It can be performed without step 1, if it is A-RAN who initiates the periodic inventory. The inventory strategy should be set to delta inventory.
3. The AIOT device responds if it hasn’t been “inventoried”. Using the reader identity information (e.g. A-RAN ID) over the air, AIOT device determines if it is being read by a new A-RAN node and responds the inventory. The device may provide CN allocated device ID if it received before.

6. Can be skipped if the AIOTF finds AIoT device has performed the authentication and authorization with the network, based on CN allocated device ID.

7. Can be skipped if the AIOTF decides not to allocate a new CN allocated device ID by local policy.

8. Can be skipped if the AIOTF has registered towards UDM.

9. The AIOTF may use the aggregation period provided by the AF, or a locally configured value or even skip the aggregation, based on local policy. If the AIoT device responds the inventory procedure due to the A-RAN is a new reader, the device ID may not be sent to AF via NEF, unless AF requires the location information.

10. The AIOTF sends Inventory Notify Request towards the NEF for the device ID or the aggregated device ID information.

11. The NEF sends Inventory Notify Request towards the AF for the device ID or the aggregated device ID information.

### 6.8.3 Impacts on services, entities and interfaces

Editor's note: The services, entities and interfaces are FFS.

## 6.9 Solution #9: Information Transfer without a PDU Session

### 6.9.1 Description

This solution is to address the KI#1, KI#2 and KI#3. This solution is to support the DO-DTT and DT traffic type and an enhancement to the 5GS to support the AIoT Device. The main points are as following:

- The AIoT Device still performs the initial registration procedure, and after the initial registration procedure, the AMF can set up the transmission tunnel towards the AIoT NF; No PDU Session has been established at the AIoT device and the CN. No mobility registration update registration procedure is performed. During the registration procedure, a temporary ID is allocated to the AIoT Device for the security reason.

- There is no CM state at the AIoT Device or the AMF. After the initial registration procedure, there is no active NAS connection maintained between the AIoT Device and the AMF; however the AIoT Device and the AMF require to maintain MM context.

- For the DT traffic (e.g command from the AF) over the air interface, the RAN can perform paging (or paging like);

- For the DO-DTT traffic (e.g feedback or the DO-DTT data reporting to the AF), it can be sent over the NAS;

- If the AF is in the 3rd party domain, the NEF function can be combined into the AIoT NF.

Figure 6.9.1-1 shows the 5GS enhancement to support AIoT Device.



Figure 6.9.1-1 5GS enhancement to support AIoT Devices

### 6.9.2 Procedures

Figure 6.9.2-1 shows the signalling flow for the DT traffic (e.g command) delivery and DO-DTT data reporting.



Figure 6.9.2-1 Signalling flow for Information Transfer

1. AF performs the service configuration. This service configuration can provide the AIoT Device ID(s) information to the AIoT NF. The AIoT NF can further provide the AIoT Device ID information to the UDR.

2. The AIoT Device performs the AS procedure.

Editor's Note: Whether and how to trigger the AS procedure is to be studied in RAN WGs and to be defined in TR 38.769 [8].

3. The AIoT Device performs the Initial registration procedure. In this step, the AIoT Device ID is included in the Registration Request.

Editor's Note: whether to reuse the initial registration procedure defined in TS 23.502 [5] or to define a new registration procedure is FFS.

Editor's Note: The format of AIoT Device ID is FFS and how to protect the Device ID is FFS.

4. The AMF performs the Device ID validation by retrieving the subscription data from the UDM. The subscription data can also include the AIoT NF information.

Editor's Note: The validation of AIoT Device requires coordination with SA3.

Editor's Note: Whether the UDM has the subscription data per Device ID or group of Devices or other granularities is FFS.

Editor's Note: It is FFS whether it can be assumed that the device and the CN can be pre-provisioned with CN level per device information (e.g. network layer AIoT device ID, security material).

5-6. The AMF sets up a transmission tunnel towards the AIoT NF. And the AIoT NF acks this setting up procedure. Multiple AIoT devices can share this transmission tunnel.

Editor's Note: The concept of transmission tunnel, how to set up the transmission tunnel and what is the granularity of the transmission tunnel is FFS.

7. The AMF accepts the registration procedure if the AIoT Device has been validated. The AMF also allocates a temporary id to the AIoT Device in the Registration Accept message.

8. AF delivers the command to the AIoT NF including the Device ID(s) and detailed "Command" information.

9. AIoT NF forwards the AIoT Device ID information and detailed "Command" information to the AMF.

10. Since the AMF does not maintain the CM state for the AIoT Device, the AMF utilizes the RAN information where the AMF receiving the N2 message for the AIoT Device for paging. The paging (or paging-like) includes the temporary ID and detailed "Command" information. The AMF sends paging to the RAN and RAN performs the paging over the air interface.

Editor's Note: How to protect the detailed "Command" information is FFS.

Editor's Note: The paging (or paging-like) requires coordination with RAN WGs.

11. The AIoT Device checks the temprory ID in the paging message and if the tempory ID is matched, the AIoT Device then handles "Command". If feedback or DO-DTT (e.g. sensor data reporting) is required, the AIoT Device includes DO-DTT traffic over the NAS.

12. The AMF forwards the DO-DTT traffic to the AIoT NF;

13. The AIoT NF forwards the DO-DTT traffic to the AF.

### 6.9.3 Impacts on services, entities and interfaces

Editor's Note: The impacts on services, entities and interfaces are FFS.

## 6.10 Solution #10: Registration procedure for Ambient IoT Devices

### 6.10.1 Description

This solution is for Key Issue #2 "Identification, Subscription, Registration and Connection management".

As depicted in Architecture Requirements, the traffic types of DT and DO-DTT will be studied in this stage. The Ambient IoT devices could be driven by the network for Topology1 or UE for topology 2 before registering to the network. This proposal proposes one potential mechanism for identification, subscription, registration management and the registration procedures as well.

The principles/assumptions are given below:

- A new network function named Ambient IoT NF may be adopted to manage Ambient IoT devices and procedures. If not, this relevant function can be supported by AMF.

- In 5GC, each Ambient IoT device has a unique internal ID which consists of at least Operator ID, and Company. Optionally, the group ID in terms of the client or the type of item may be contained in the device ID.

- The solution is based on an operator-controlled Ambient IoT device.

### 6.10.2 Procedures

#### 6.10.2.1 Procedures for AF triggered Registration

The following figure presents a procedure of AF triggered registration for Topology 1.

5. AF Triggered Registration Request (TID lists, EPC info …)

8. AF Triggered Registration Response

10. AF Triggered Registration Response

1. AF Triggered Registration Request ( TID Lists, EPC info lists, Location, …)

2. AMF or New Ambient IoT NF selection

9. AF Triggered Registration Response

3. AF Triggered Registration Request (TID lists, TA Lists, EPC info …)

AMF or New

Ambient IoT NF

Ambient AF

fd

AAA

NEF

Ambient IoT Device

1. Pre-configuration

4. NG-RAN Selection

6. Device Access

7. Authentication and Registration

UDM

NG-RAN

Figure 6.10.2-1 AF triggered Registration Procedure for Topology 1

0. The Ambient IoT devices are pre-configured with default internal AIoT device ID and credentials.

The 5GC is pre-configured with the default Ambient IoT devices profile which contains the device ID and credentials too. The default internal AIoT device ID only contains Operator ID and Company info, without product info, serial number, and so on.

Editor’s note: the information contained in Operator ID is FFS.

Editor’s note: it is FFS whether it can be assumed for all scenarios that the device and CN can be pre-provisioned with CN level per device information (e.g. network layer AIoT device ID, security material).

1. AF triggers registration and sends AF Triggered Registration Request to NEF. The service information such as the EPC code list (See GS1 TDS Release 2.1 [10]), TID code list (See GS1 TDS Release 2.1 [10]), and location information are included.

Editor’s note: Clarification on how to use TID and EPC are FFS.

2. The NEF selects an AMF or Ambient IoT NF that supports Ambient IoT services based on the location information. It will map the location information into the TA list.

3. The NEF sends AF Triggered Registration Request to the AMF/Ambient IoT NF, including the TID list, EPC info, and the TA list.

4. The AMF/Ambient IoT NF selects NG-RAN based on the TA list.

5. The AMF/Ambient IoT NF forwards the registration request to NG-RAN, including the TID list, EPC info, and so on.

6. NG-RAN activates the AIoT devices based on TID list. The devices matched TID list access and register to the network via NG-RAN with EPC info. A receiving limit time may be configured on NG-RAN. Once timeout, the message received after this time will be discarded by NG-RAN.

7. The AIoT devices perform interaction with 5GC for Authentication/Security. After successful registration, 5GC will generate a full internal AIoT device ID, containing the Operator ID, Company info, product info, and serial number based on EPC info.

Editor’s note: whether to store the full internal Ambient IoT device ID with EPC info in 5GC is FFS

8. The NG-RAN returns the Response to the AMF/Ambient IoT NF.

9. The AMF/Ambient IoT NF returns the response to the NEF.

10. The NEF returns AF Triggered Registration Response to the AF.

#### 6.10.2.2 Procedures for UE triggered Registration

For Topology 2, the registration may be triggered by UE which performs as a reader. The UE interact with AMF or Ambient IoT NF via NG-RAN, which could be regarded as the supplement for AF triggered registration procedure.

Editor’s Notes: The procedure for UE triggered registration is FFS.

### 6.10.3 Impacts on services, entities and interfaces

NEF:

- The NEF supports conversion between the internal AIoT device ID and EPC code.

AMF/Ambient IoT NF:

- The AMF/Ambient IoT NF selects NG-RAN based on the TA list or gNB list and activates the AIoT devices.

UDM:

- The UDM stores the subscription information of Ambient IoT devices in group.

NG-RAN as a reader:

- The NG-RAN performs paging and receives response of Ambient IoT devices in Topology 1.

UE as a reader:

- The UE performs paging and receives response of Ambient IoT devices in Topology 2.

- The UE supports to trigger the registration procedure.

Ambient IoT device:

- The device stores the internal AIoT device ID or the group ID.

## 6.11 Solution #11: 5GC support for AF to retrieve data from AIoT devices

6.11.1 Description

This solution address aspects of key issue #3 on Support of Ambient IoT Services.

This solution enables the AF to retrieve data from the target AIoT devices via 5GC, using Topology 2.

Editor's note: it is FFS whether the proposed solution can be applied for Topology 1, and whether the same interface can be used between AIoT device and AIoTF for both Topology 1 and 2.

This solution considers scenarios in which an application service provider has prior information about intermediate nodes (abbreviated as I-node) expected to be located in specific places (e.g., intermediate nodes being used only in particular warehouses). Additionally, scenarios where the provider knows candidate locations for the target AIoT devices (e.g., the AIoT devices attached to goods are expected to be in particular warehouses or retail markets) are also considered.

The assumption and high-level procedures of this solution are as follows:

- The AIoT device ID is defined by the external application and provided by the AF to the 5GC when requesting the AIoT-related services. The uniqueness of the AIoT device ID per application is assumed to be guaranteed by the application itself, while achieving the uniqueness of the AIoT device ID in the 5G domain could be accomplished, for example, by prefixing the unique owner ID (e.g., unique company prefixes assigned by EPCglobal).

Editor's note: How to ensure the uniqueness of the AIoT device ID is FFS.

- AIoT devices are not registered with the 5GC.

- A UE, additionally capable of directly communicating with the AIoT devices, is acting as the intermediate node.

- A UE acting as an intermediate node is registered with 5GC using the existing mechanism, with some enhancements to indicate its capability of acting as an intermediate node.

- The AF possesses information about the candidate location(s) of the target AIoT devices or about the preferred intermediate node (i.e., external UE ID) and provides them when requesting the AIoT related services to 5GC.

- When information about the preferred intermediate node is provided while it is not operational, or when the location(s) of the target AIoT devices are given, the 5GC selects the intermediate node based on the network information. The process of selecting such an intermediate node is not within the scope of this solution. This means that this solution supports both static and dynamic binding with the intermediate node.

- How to support security between each entity (e.g., between AIoT device and I-node, and AIoT device and CN) involved in the procedures (e.g., relying on application security or providing network security based on the information provided by the application) is assumed to be addressed by SA3.

- The Uu interface between the intermediate node and the gNB is assumed to be used, while a new protocol stack, defined by RAN, is assumed to be used between the AIoT device and the intermediate node.

6.11.2 Procedures

The procedure for data retrieval from AIoT devices based on AF request is depicted in figure 6.11.2-1.



Figure 6.11.2-1: Information Flow for AIoT data retrieval

To facilitate communication between an external AF with AIoT devices for data retrieval, this solution proposes certain measures to be taken:

0. It is assumed that the AF requesting 5GC to retrieve data from specific AIoT devices possesses their AIoT device IDs, either defined by the device manufacturer or the AF itself, along with candidate locations of the AIoT devices or information (e.g., external ID) of the intermediate node covering the target AIoT devices.

1. The intermediate node is a UE with the capability to directly communicate with the AIoT devices. The intermediate node is registered with the 5GC. They may indicate support of the capability to act as an intermediate node.

2. The AF sends a request to 5GC, utilizing an API called AIOT\_Read, to read data from the target AIoT devices. The AF’s request includes following parameters: the target AIoT device IDs defined by the external application and installed in the AIoT devices, the candidate locations of the target AIoT devices or the external ID (i.e., external UE ID) of the intermediate node that can directly communicate with the target AIoT devices, optionally specific target data to be read by the AF.

3. Upon receiving the AF request, the NEF authorizes the AF request based on SLA.

4. The NEF translates the external ID (e.g., GPSI) of the intermediate node, if provided, to the SUPI via UDM and verifies whether the UE possessing the translated SUPIs is authorized to function as intermediate node through UDM. The NEF translates the location, if provided by the AF, into 3GPP based location information (Tracking areas TA(s), cell ID(s), etc). The NEF identifies the serving AMF(s) via UDM by utilizing the SUPI of the intermediate node, if applicable, or by considering the candidate locations of the AIoT devices. The NEF selects AIoTF that can be a standalone NF or collocated with the NEF.

5. An AIOT\_Read request message is sent to the AIoTF, including the following parameters: the target AIoT devices, candidate locations or the SUPI of the intermediate node, Serving AMF(s) as derived in step 4, optional Requested target data.

6. The AIoTF may select the intermediate node based on the information provided in step 5 to communicate with the target AIoT devices.

Editor's note: It is FFS how the intermediate node is selected by the CN or the gNB based on the location information.

7. The AIoTF requests the serving AMF to initiate the communication, which includes the target AIoT device IDs, candidate locations or SUPI of the selected intermediate node, and optional Requested target data.

8. The AMF identifies the serving gNB by utilizing the SUPI of the intermediate node, if applicable, or by considering the candidate locations of the AIoT devices.

9. The gNB may select the intermediate node, if not provided in step 8, based on the local RAN conditions to communicate with the target AIoT devices, which is beyond the scope of this solution.

10. The gNB requests the selected intermediate node to read the AIoT data, providing the target AIoT device IDs and the Requested target data (if applicable).

11. The selected intermediate node sends out a request which includes the target AIoT device IDs and the Requested target data (if applicable).

12. The AIoT devices check whether their device IDs match any of the target AIoT device IDs included in the received request. If there's no match, the AIoT devices do not react.

13. If there’s a match, the AIoT devices check the presence of Requested target data within the request. If it is absent, the AIoT devices send a response message incorporating only their device IDs. If the Requested target data is present, the AIoT devices send a response message including their device IDs and only the data requested to the intermediate node.

14. The intermediate node receives the response message from the AIoT devices. If the AIoT device ID within the received message corresponds to any of the target AIoT device IDs obtained in step 10, the intermediate node assesses which AIoT devices, from the list of expected AIoT devices, have provided a response. The intermediate node then forwards this information, encompassing AIoT device data (if applicable) and the AIoT device ID, to the AF possibly via gNB, AMF, AIoTF and NEF. How exactly the intermediate node forwards the received information and the requirement for 5GC awareness of the UL traffic are beyond the scope of this solution.

6.11.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing services, entities and interfaces.

## 6.12 Solution #12: UE Function Delegation in Intermediate Node for AIoT Device

### 6.12.1 Description

This solution applies to those AIoT devices that are not capable of direct communication with a 5G network, and instead, may communicate with the network through an Intermediate Node (IN), or “IN-UE”. The AIoT device and the IN-UE may communicate with each other using backscattering communication or other sidelink technologies. It is assumed that the AIoT device is able to identify itself, e.g., using its Device Identifier, over the “AIoT device – UE” interface.

NOTE 1: How the AIoT device communicate with the IN-UE is not in the scope of this solution.

The general principles of this solution are:

For a AIoT device or a group of AIoT devices that the IN-UE acts as Intermediate Node, the IN-UE instantiates a “UE Function Delegation Module” (UFDM) which represents the AIoT device and appears as a “UE” towards the 5GC. It is also referred to as “UFDM-UE” in this solution. The instantiation may be initiated after the IN-UE has been authorized as the IN. The AIoT device(s) for which the IN-UE acts as the IN may be preconfigured in the IN-UE or obtained during the IN authorization procedure.

NOTE 2: The IN authorization procedure is not covered by this solution.

After a new UFDM is instantiated, the IN-UE initiates an “AIoT device provisioning” procedure with the 5GC and through this procedure the UFDM is allocated a temporary UE identifier, e.g. a temporary SUPI, associated credentials, and other necessary configuration and policies (e.g., URSP policy). A UFDM maintains its own NAS connection and registration state with the 5GC. The UFDM-UE’s NAS connection and IN-UE’s NAS connection share the IN UE’s RRC connection and the UFDM’s NAS messages may be sent as payload of IN UE’s NAS messages.

Though from the perspective of the network, a UFDM functions as a separate UE, the 5GC maintains the association between the intermediate node UE and other “UE(s)” represented by the UFDM(s) residing inside the intermediate node UE, so the network can optimize some procedures, e.g. paging procedure.

The IN UE maintains the association between the UFDM and the AIoT device and manage the lifecyle of the UFDM. For example, when the IN-UE detects that the AIoT device is not responding to the Command or activation signal, the corresponding UFDM instance may be deactivated and the 5GC may also be informed. In that case, the previously provisioned UE identifiers and credentials for the UFDM-UE is invalidated.



Figure 6.12.1-1: UFDM in AIoT Capable UE for AIoT devices

The UFDM handles the data forwarding between its associated AIoT device and the network. For example, the UFDM may use Control Plane 5GS Optimization for CIoT mechanism to forward AIoT device data to the application server or vice versa.

### 6.12.2 Procedures

#### 6.12.2.1 UFDM instantiation and provisioning



Figure 6.12.2.1-1: UFDM instantiation and provisioning

1. The IN-UE is authorized as a IN. This may happen during the IN-UE Registration based on IN-UE capabilities and subscription information. The AIoT devices that the IN-UE can act as IN may be preconfigured in the UE and provided by the network during the authorization procedure.

2. The UFDM instantiation in the IN UE is triggered by Step 1. For each device that the UE can act as IN, The IN UE creates a UFDM instance, allocates a UFDM instance ID and associate it with the AIoT device.

3. The IN UE initiates AIoT Device Provisioning Request towards the 5GC UDM and includes the AIoT device identifier in the request. If the IN UE is preconfigured with default credentials for the AIoT device, it may also include the default credentials in the request.

4. The UDM validates the AIoT device ID and default credentials (if available). If necessary, the UDM may interact with external servers via NEF to complete the validation process.

NOTE: How the device ID and credential is validated is not covered in this solution.

Editor's note: The details of the provisioning procedure (Step 3 and 4) are FFS and the security aspects may need SA3 study.

5. If the AIoT device is valid, the UDM allocates a temporary SUPI, associated credentials (e.g. AKA keys) and provide them to the IN UE in the response message. Other necessary configuration and policies, e.g. URSP rules, default QoS rule, etc. may also be provided.

6. The IN UE stores the received information as the UFDM context.

#### 6.12.2.2 UFDM Registration

UFDM acts as a separate “UE” towards the network so it performs Registration procedures similar to what a normal UE would do. However, to avoid unnecessary signalling, some of the UFDM’s Registration procedures (e.g. periodical Registration update or mobility Registration update) may be combined with the IN UE’s own Registration procedures.



Figure 6.12.2.2-1: UFDM registration

1. The UFDM-UE NAS sends a “Registration Request” to the IN-UE NAS. The UFDM-UE may use the SUPI that’s obtained through the provisioning procedure as the initial UE identifier.

2. If the IN-UE is not already in CM-CONNECTED state, it initiates the signalling procedure to enter CM-CONNECTED state, then it sends the UFDM-UE’s Registration Request as the payload of its own NAS message, e.g. UL Transport, to the serving AMF.

3. The AMF and other NFs handles the UFDM-UE’s Registration request as described in TS 23.502 [5]-clause 4.2.2.2.2.

4. The AMF sends the Registration Accept as the payload of the IN-UE’s NAS message, e.g., DL Transport.

5. The AMF associate the UFDM-UE identifier with the IN-UE identifier. By maintaining this association, the AMF is able to target the IN-UE as the recipient for signalling/data of the UFDM-UE.

6. The IN-UE forwards the Registration Accept message to the UFDM-UE.

### 6.12.3 Impacts on services, entities and interfaces

UE:

- Supports UFDM instantiation and management.

- Supports forwarding UFDM NAS signalling as payload of IN UE NAS messages.

- Supports AIoT data forwarding as UFDM data.

AMF:

- Supports handling UFDM NAS messages as IN NAS payload.

- Supports handling AIoT Device Provisioning procedure.

- Supports maintaining association between UFDM UE and IN UE.

UDM/UDR

- Supports validation of AIoT device identifier and credential.

- Supports AIoT Device Provisioning.

## 6.X Solution #X: <Solution Title>

### 6.X.1 Description

Editor's note: This clause will describe the solution principles and architecture assumptions for corresponding key issue(s). Sub-clause(s) may be added to capture details.

### 6.X.2 Procedures

Editor's note: This clause describes high-level procedures and information flows for the solution.

### 6.X.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing services, entities and interfaces.

# 7 Overall Evaluation

Editor's note: This clause will provide a general evaluation and comparison of the solutions per Key Issue #<X>.

# 8 Conclusions

Editor's note: This clause will capture conclusions for the study.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-01 | SA2#160AH-e | S2-2400509 | - | - | - | Proposed skeleton agreed at SA2#160AH-e | 0.0.0 |
| 2024-01 | SA2#160AH-e | - | - | - | - | Inclusion of documents approved in SA2#160AH-e:  S2-2401820, S2-2401821, S2-2401822, S2-2401823, S2-2401824, S2-2401825, S2-2401840. | 0.1.0 |
| 2024-03 | SA2#161 |  |  |  |  | Inclusion of documents approved in SA2#161:  S2-2403137, S2-2403140, [S2-2403427](E:\\3GPP会议\\SA2\\SA2#161_Athens24\\Agreed_AIoT_PCRs_161\\Docs\\S2-2403427.zip), [S2-2403719](E:\\3GPP会议\\SA2\\SA2#161_Athens24\\Agreed_AIoT_PCRs_161\\Docs\\S2-2403719.zip), [S2-2403429](E:\\3GPP会议\\SA2\\SA2#161_Athens24\\Agreed_AIoT_PCRs_161\\Docs\\S2-2403429.zip), S2-2403430, S2-2403431, [S2-2403469](E:\\3GPP会议\\SA2\\SA2#161_Athens24\\Agreed_AIoT_PCRs_161\\Docs\\S2-2403469.zip), [S2-2403471](E:\\3GPP会议\\SA2\\SA2#161_Athens24\\Agreed_AIoT_PCRs_161\\Docs\\S2-2403471.zip), S2-2403472, S2-2403473, S2-2403474, S2-2403475, S2-2403720, S2-2403721, S2-2403722 . | 0.2.0 |