|  |  |
| --- | --- |
| 3GPP TR 23.700-13 V0.3.0 (2024-04) | |
| 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 7

1 Scope 9

2 References 9

3 Definitions of terms and abbreviations 9

3.1 Terms 9

3.2 Abbreviations 10

4 Architectural Assumptions and Requirements 10

4.1 Architectural Assumptions 10

4.2 Architectural Requirements 11

5 Key Issues 11

5.1 Key Issue #1: Architecture support of Ambient IoT Devices 11

5.1.1 Description 11

5.2 Key Issue #2: Identification, Subscription, Registration and Connection management 11

5.2.1 Description 11

5.3 Key Issue #3: Support of Ambient IoT Services 12

5.3.1 Description 12

6 Solutions 13

6.0 Mapping of Solutions to Key Issues 13

6.1 Solution #1: AIoT Temporary Identifier Control 13

6.1.1 Description 13

6.1.2 Procedures 13

6.1.3 Impacts on services, entities and interfaces 14

6.2 Solution #2: AIoT Device ID with home network, owner and instance identification 14

6.2.1 Description 14

6.2.2 Procedures 16

6.2.3 Impacts on services, entities and interfaces 16

6.3 Solution #3: Lightweight Ambient IoT system 16

6.3.1 Description 16

6.3.1.1 Introduction 16

6.3.1.2 Definitions 16

6.3.1.3 Assumptions 17

6.3.1.4 Reference architecture 17

6.3.1.5 Network function description 17

6.3.1.5.1 Reader 17

6.3.1.5.2 AIoT Controller 18

6.3.1.5.3 AF 18

6.3.1.6 Protocol Stacks 19

6.3.1.6.1 Protocol Stack between Reader and AIoT Controller 19

6.3.1.6.2 Protocol Stack between AIoT Device and Application Function 20

6.3.2 Procedures 21

6.3.2.1 Inventory procedure 21

6.3.2.2 Command procedure 23

6.3.3 Impacts on services, entities and interfaces 24

6.4 Solution #4: Simplified system for AIoT 24

6.4.1 Description 24

6.4.1.1 General 24

6.4.1.2 Abbreviations 24

6.4.1.3 Terms 24

6.4.1.4 Reference Architecture and NFs 25

6.4.1.5 Protocol Stack 26

6.4.2 Procedures 27

6.4.2.1 Inventory procedure 27

6.4.2.2 Command procedure 28

6.4.3 Impacts on services, entities and interfaces 29

6.5 Solution #5: NAS-based information transfer for Ambient IoT Services 29

6.5.1 Description 29

6.5.2 Procedures 29

6.5.3 Impacts on services, entities and interfaces 31

6.6 Solution #6: AIoT device authentication, ID validation and AIoT communication 31

6.6.1 Key Issue mapping 31

6.6.2 Functional Description 31

6.6.3 Procedures 33

6.6.4 Impacts on existing services, entities and interfaces 36

6.7 Solution #7: Bulk Introduction of Devices to the Network 36

6.7.1 Description 36

6.7.2 Procedures 37

6.7.3 Impacts on services, entities and interfaces 37

6.8 Solution #8: Inventory for AIoT Devices using AIOTF 38

6.8.1 Description 38

6.8.2 Procedures 40

6.8.2.1 Application Inventory Procedure 40

6.8.2.2 Periodic Inventory Procedure 43

6.8.3 Impacts on services, entities and interfaces 44

6.9 Solution #9: Information Transfer without a PDU Session 44

6.9.1 Description 44

6.9.2 Procedures 45

6.9.3 Impacts on services, entities and interfaces 46

6.10 Solution #10: Registration procedure for Ambient IoT Devices 46

6.10.1 Description 46

6.10.2 Procedures 47

6.10.2.1 Procedures for AF triggered Registration 47

6.10.2.2 Procedures for UE triggered Registration 48

6.10.3 Impacts on services, entities and interfaces 48

6.11 Solution #11: 5GC support for AF to communicate with AIoT devices 49

6.11.1 Description 49

6.11.2 Procedures 50

6.11.2.1 Communication with AIoT devices 50

6.11.2.2 Selection of intermediate nodes 52

6.11.3 Impacts on services, entities and interfaces 55

6.12 Solution #12: UE Function Delegation in Intermediate Node for AIoT Device 55

6.12.1 Description 55

6.12.2 Procedures 57

6.12.2.1 UFDM instantiation and provisioning 57

6.12.2.2 UFDM Registration 58

6.12.3 Impacts on services, entities and interfaces 59

6.13 Solution #13: Multi-level Device ID management 59

6.13.1 Description 59

6.13.2 Procedures 59

6.13.3 Impacts on services, entities and interfaces 60

6.14 Solution #14: AIoT Device ID with consideration on credential holder, service provider and mobile network 60

6.14.1 Description 60

6.14.2 Procedures 61

6.14.3 Impacts on services, entities and interfaces 64

6.15 Solution #15: Ambient IoT Device States 64

6.15.1 Description 64

6.15.1.1 Overview 64

6.15.1.2 New AIoT Device States 64

6.15.2 Procedure for State Toggling in AIoT Devices 65

6.15.3 Impacts on services, entities and interfaces 67

6.16 Solution #16: AIoT Registration/Onboarding 67

6.16.1 Description 67

6.16.2 Procedures 68

6.16.3 Impacts on services, entities and interfaces 69

6.17 Solution #17: Enable Ambient IoT Management within 5GC to support AIoT services 70

6.17.1 Description 70

6.17.1.1 General 70

6.17.1.2 Architecture Principles 70

6.17.1.3 Function Principles 71

6.17.2 Procedures 73

6.17.2.1 General 73

6.17.2.2 AIoT Service High-Level Information Flow 73

6.17.2.3 NEF AIoT Service 76

6.17.3 Impacts on services, entities and interfaces 77

6.18 Solution #18: Solution for support of Ambient IoT services 77

6.18.1 Description 77

6.18.2 Procedures 78

6.18.2.1 Ambient IoT service --- Network initiated Ambient IoT service procedure 78

6.18.3 Impacts on services, entities, and interfaces 81

6.19 Solution #19: AIoT communication for connectivity topology 1 82

6.19.1 Key Issue mapping 82

6.19.2 Functional Description 82

6.19.3 Procedures 83

6.19.3.0 General 83

6.19.3.1 N2' association establishment 83

6.19.3.2 AIoT session establishment between the AIoTF and the AIoT AF/AS and AIoTF and the BS AIoT Reader 85

6.19.4 Impacts on existing services, entities and interfaces 87

6.20 Solution #20: E2E handling for interaction of AIoT Device related information 87

6.20.1 Description 87

9.3.3.1 AMF UE NGAP ID 88

9.3.3.2 RAN UE NGAP ID 88

6.20.2 Procedures 90

6.20.2.1 The interaction for AIoT Device among AIoT device, reader and AIoT Function 90

6.20.2.2 The interaction for AIoT Device among AIoT device, reader, AIoT Function and AF. 91

6.20.3 Impacts on services, entities and interfaces 93

6.21 Solution #21: Architecture enhancement to support AIoT services for topology 2 93

6.21.1 Description 93

6.21.2 Procedures 94

6.21.3 Impacts on services, entities and interfaces 96

6.22 Solution #22: AF Based Solution for Topology 2 96

6.22.1 Description 96

6.22.1.0 General 96

6.22.1.1 Reference Architecture 96

6.22.1.2 Protocol Stack 97

6.22.2 Procedures 98

6.22.2.1 AIoT Service Authorization for Intermediate UE 98

6.22.2.2 Inventory Procedure 99

6.22.2.3 Command Procedure 100

6.22.3 Impacts on services, entities and interfaces 102

6.23 Solution #23: UE reader selection for inventory procedure 102

6.23.1 Description 102

6.23.1.1 Definition 102

6.23.1.2 General 102

6.23.1.3 Architecture and Principles 103

6.23.2 Procedures 103

6.23.3 Impacts on services, entities and interfaces 104

6.24 Solution #24: Availability Reporting without Ambient IoT Device Timers 105

6.24.1 Functional Description 105

6.24.2 Procedures 105

6.24.3 Impacts on existing services, entities and interfaces 107

6.X Solution #X: <Solution Title> 107

6.X.1 Description 107

6.X.2 Procedures 107

6.X.3 Impacts on services, entities and interfaces 107

7 Overall Evaluation 108

8 Conclusions 108

Annex A: Overview of the Electronic Product Code 108

Annex B: Change history 110

# 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".

[11] GS1 Organisation: The Global Language of Business. Available at: https://www.gs1.org/

[12] GS1: Standards in the Healthcare Supply Chain. Available at: https://www.gs1.ch/de/media/1117

[13] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[14] 3GPP TS 38.401: "NG-RAN; Architecture description".

# 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.

**Electronic Product Code:** A universal identifier that provides a unique identity for any physical object as defined by GS1 in the EPC Tag Data Standard [10] and used for identification needs of various business domains.

## 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

EPC Electronic Product Code

RFID Radio-Frequency IDentification

# 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 |
| #13 |  | X |  |
| #14 |  | X |  |
| #15 |  | X | X |
| #16 |  | X |  |
| #17 | X | X | X |
| #18 |  |  | X |
| #19 | X |  | X |
| #20 | X | X | X |
| #21 | X | X | X |
| #22 | X | X | X |
| #23 |  |  | X |
| #24 |  | 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 initial 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 SA WG3.

- If 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 algorithm.

- 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. Filter Criteria may consist of the following:

- an EPC as defined by GS1 in the EPC Tag Data Standard [10] and optionally a bitmask.

Editor's note: Other Filter Criteria are FFS.

NOTE: The term Filter Criteria can be revisited to avoid clashes with existing terminology.

- **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 SA WG3.

- 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. The EPC as defined by GS1 in the EPC Tag Data Standard [10] is used as the Device ID.

NOTE 2: Whether also dynamic (re-)provisioning of Ambient IoT Devices can be supported is up to SA WG3.

- The radio configuration (frequency bands, etc.) of the Reader is assumed to be configured through an OAM system, which is beyond the scope of SA WG2.

#### 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 RAN WG3.

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.

Figure 6.3.1.6.2-1

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;

NOTE: If the AF does not provide Filter Criteria, then a full inventory of all AIoT devices reachable by the Reader(s) will be performed.

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

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

As part of the Filter Criteria an AF may provide an EPC and optionally a bitmask. This enables the AF to trigger a targeted inventory:

- For example, an AF may want to inventory complete shipments only (identified by AIoT devices attached to the pallets that carry the shipment), without having to unnecessarily inventory also all AIoT devices which may be located on the pallets. This can be achieved by limiting the inventory to AIoT devices that carry an EPC based on the Serial Shipping Container Code EPC scheme. To do so, the AF may provide a bitmask that only matches on the Header value of the EPC and an EPC value that contains the standardized Header value for the Serial Shipping Container Code EPC scheme. (See Annex X for further details on EPC schemes and EPC Header values.).

- Another example is an AF that may only want to inventory individual items from a specific company. This can be achieved by limiting the inventory to AIoT devices that carry an EPC that is based on the Serialised Global Trade Item Number (SGTIN) EPC scheme and where the GS1 Company Prefix contained in the SGTIN matches the company prefix of the specific company that the AF is interested in. To do so, the AF may provide a bitmask matching on the Header value of the EPC and the bits of the GS1 Company Prefix contained in the Serialised Global Trade Item Number (SGTIN) EPC scheme and may provide an EPC that contains the standardized Header value for the Serialised Global Trade Item Number (SGTIN) and the Company Prefix value of the company that the AF is interested in.

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. If the Filter Criteria contain an EPC and optionally a bitmask, then the Reader sends the EPC and the bitmask as part of the inventory request. The Readers either perform a one-time inventory or perform the inventory periodically according to the received periodicity.

5. If the Inventory Request contains an EPC, then the AIoT Device compares the received EPC with its Device ID, i.e., the locally stored EPC. If the Inventory Request also contains a bitmask, then the AIoT Device only compares the relevant bits according to the bitmask. If the Inventory Request does not contain an EPC, then the AIoT Device skips this step.

6. If the Inventory Request contains an EPC and optionally a bitmask, and the received EPC matches the locally stored EPC (or parts of the EPC in case a bitmask was provided) as described in the previous step, then the AIoT Device responds to the Reader.

If the Inventory Request does not contain an EPC, then the AIoT Device responds to the Reader.

NOTE: The AIoT Device responds to Inventory Requests that do not contain an EPC to enable the case that an AF wants to perform a full inventory.

The AIoT Device includes its Device ID in the Inventory Response.

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

8. 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.

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

NOTE: The AIoT Controller provides the Device IDs as received to the AF, i.e., the AIoT Controller is not assumed to verify Device IDs.

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 SA WG3.

### 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 SA WG2 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 topology 1 & 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 alternative 1



Figure 6.4.1.4-3: The example of reference architecture for alternative 2

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 SA WG3.

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 SA WG3.

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 of a group of devices (e.g. configured in the UDM/UDR and AIoT devices). 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 ID and corresponding credentials are used for the security protection of the group ID and AIoT data destined to the group ID. The group of devices can be organized by sharing the same service, so the group 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 or a group of AIoT devices. 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, AIOT service policy (priority for the AIOT data transmission, service duration, periodic transmission frequency if it’s periodic transmission, aggregation waiting time for group transmission if the communication is for a group of AioT devices), 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 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.

- AIOT service policy includes destination transmission area, priority, service duration (e.g., start and stop time) , periodic transmission frequency during the service duration if it’s periodic transmission, 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. When the AIoT service duration time starts if those parameters are presented in step 5, 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, optional group ID if group ID is included in the DL AIoT data/signalling 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, optional group ID if group ID is included in the DL AIoT data/signalling, 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, or Group ID, and/or UL MAuC using the credentials for the individual device ID (e.g. received in step 2b) or group ID.

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. If the AIoT report includes group ID, AIoT-GW performs aggregation and buffering the UL data of the devices with the same group ID during the aggregation waiting time provided by the AF/AS. When the aggregation waiting time expires, the AIOT-GW sends the UL reports of those AIoT devices belonging to the same group.

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-GW can support the functionality to aggregate the UL data of the devices with the same group and provide the aggregated data to the AF.

- 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 SA WG5.

- 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 SA WG3.

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.



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 note: 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 communicate with 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 communicate with the target AIoT devices for DO-DTT and DT traffic types via 5GC, dedicated for only Topology 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, such as by adhering to standards like EPC (Electronic Product Code) and utilizing EPCglobal allocation, which manages a global registry for unique prefixes among different companies..

- AIoT devices are not registered with the 5GC.

- AIoT Devices are provisioned with AIoT Device ID and associated security materials.

- 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, and is authorized as an intermediate node (UE) during the registration procedure.

- 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.

- If the AF is in the 3rd party domain, the AF can communicate with the 5GC via NEF that can be combined with the AIoT NF.

- 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 SA WG3.

- 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.

- For DO-DTT traffic (e.g response from the AIoT device to the network), it can be sent over the NAS of the intermediate node.

Figure 6.11.1-1 shows the 5GS enhancement to support AIoT Device.



Figure 6.11.1-1 5GS enhancement to support AIoT Devices for Topology 2

### 6.11.2 Procedures

#### 6.11.2.1 Communication with AIoT devices

The procedure for communicating with AIoT devices based on AF request is depicted in figure 6.11.2.1-1.



Figure 6.11.2.1-1: 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 communicate with 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 UE performs the registration procedure as specified in clause 4.2.2.2 of TS 23.502 [5] with the following enhancement:

- The UE indicates AIoT support in the MM capability.

- The subscription data of the UE is also enhanced to indicate whether the UE is allowed to perform the AIoT operation.

- The Registration Accept message also indicates whether the UE has been authorized to perform the AIoT operation. Validity information may also be included for the AIoT operation. Validity information can be time validity information (defined by start and end times) to indicate when the UE is allowed to perform the AIoT operation or location validity information (defined by TAI or cell ID) to indicate where the UE is allowed to performed the AIoT operation.

2. The AF sends a request to 5GC to communicate with the target AIoT devices for either DT or DO-DTT traffic type. 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, "command" information (e.g., read/write), 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.

Editor's note: The procedure for cases involving multiple locations is FFS.

5. An AIOT service request message is sent to the AIoTF, including the following parameters: AIoT session ID, the target AIoT devices, candidate locations or the SUPI of the intermediate node, Serving AMF(s) as derived in step 4, "command" information (e.g., read/write), 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. The detailed procedures for selecting the intermediate node are described in clause 6.11.2.2.

Editor's note: It is FFS how and when the selected intermediate node is configured with the necessary information for communicating with the AIoT devices and the CN.

7. The AIoTF requests the serving AMF to initiate the communication, which includes AIoT session ID, the target AIoT device IDs, candidate locations or SUPI of the selected intermediate node, "command" information (e.g., read/write) 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 (i.e., a list of TAIs and cell IDs) of the AIoT devices. The AMF then requests the gNB to send a AIoT service request, which contains the target AIoT device IDs, candidate locations or UE NGAP ID of the selected intermediate node, "command" information (e.g., read/write), and optional Requested target data, to the selected I-node. The paging request message or DL NAS Transport message can be used with some extensions to convey the AMF request, for example

9. The gNB requests the selected intermediate node to communicate with the AIoT data, providing the target AIoT device IDs, "command" information (e.g., read/write), and the Requested target data (if applicable). RRC paging message can be used by the gNB to send the request to the intermediate node, for example. When RRC paging is used, the gNB may restrict the paging area only to the identified cells for optimization, if available.

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

11. 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.

12. If there's a match, the AIoT devices check the presence of Requested target data within the request as well as "command" information to check whether DT or DO-DTT traffic type is requested. In case of DO-DTT type requested, if the Requested target data 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.

13. 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 may aggregate the response messages from the AIoT devices according to the configuration information if it was provided by the CN in advance. The intermediate node then forwards this information, encompassing AIoT device data (if applicable) and the AIoT device ID(s), to the AF via gNB, AMF, AIoTF and NEF. The AMF or AIoTF may aggregate response messages from some or all of the targeted AIoT devices during the forwarding procedures..

#### 6.11.2.2 Selection of intermediate nodes

The selection of the intermediate node can be performed based on the geographical location of the target AIoT devices or the identity of the intermediate node from AF. The procedure for selection of intermediate nodes based on geographical location is depicted in figure 6.11.2.2-1.



Figure 6.11.2.2-1: Information Flow for selecting I-node based on location of target devices from AF

1-4. Step 2 to 5 in clause 6.11.2.1 are performed.

5. The AIOTF collects necessary information from relevant NFs, for I-node selection, based on the requested location info.

a. The AIOTF first discovers the UEs present in the requested location and may also retrieve the UE related information from AMF, including connection status and reachability.

Editor's note: It is FFS what granularity the UEs in proper posture can be discovered in a requested location, especially if the UEs are Idle or Inactive. (e.g. there could be too many UEs in many gNBs are involved in the requested location)

b. The AIOTF may retrieve information related to the UEs discovered in step 5a from UDM. This information enables checking, for example, whether the UEs are registered, authenticated, authorized to act as I-nodes. Additionally, the information from UDM can include the Expected UE behaviour, as described in clause 4.15.6.3 of TS 23.502 [5], that can be used to check the battery indication, stationary indication among other parameters.

c. The AIOTF may retrieve information related to the UEs discovered in step 5a from NWDAF. This information enables checking, for example, if the discovered UEs are not too much loaded to serve the devices, function well without anomalies, or will not move out of the coverage for a significant period based on the UE related analytics as specified in clause 6.7 of TS 23.288 [13].

6. The AIOTF, based on the information collected in step 5, selects a list(s) of potential I-nodes.

7. In case no I-nodes could be selected at step 6, AIOTF sends AIOT Response with the failure reason to the AF, and the subsequent steps are skipped.

8. The AIoTF requests the serving AMF to initiate the communication with the AIoT devices, which includes the target AIoT device IDs, and the selected I-node IDs.

9. The AMF forwards the AIOT read request to gNB along with the target AIOT device IDs and the selected I-node IDs.

10. The gNB performs additional validation to assess if the received I-nodes are optimal for serving the AIoT devices, considering its local conditions such as response time, etc. Subsequently, the gNB makes the final selection on the best I-node. It is also possible that the gNB does not select any of the requested I-nodes if local conditions are not satisfied.

11. The gNB may respond to the AIOTF via AMF with the final list of selected I-nodes. In case the gNB does not selection any I-node, the response may indicate there is no available UE.

The procedure for selecting intermediate nodes when I-node ID is provided in the AF request is depicted in figure 6.11.2.2-2.



Figure 6.11.2.2-2: Information Flow for selection of I-nodes based on list of I-nodes from AF

1-4. Step 2 to 5 in clause 6.11.2.1 are performed.

5. The AIOTF collects necessary network information related to the requested UEs from relevant NFs.

a. The AIOTF may retrieve information related to the requested UE from UDM. This information enables checking, for example, whether the UEs are registered, authenticated, authorized to act as I-nodes. Additionally, the information from UDM can include the Expected UE behaviour, as described in clause 4.15.6.3 of TS 23.502 [5], that can be used to check the battery indication, stationary indication among other parameters.

b. The AIOTF may retrieve information related to the requested UE from NWDAF. This information enables checking, for example, if the discovered UEs are not too much loaded to serve the devices, function well without anomalies, or will not move out of the coverage for a significant period based on the UE related analytics as specified in clause 6.7 of TS 23.288 [13].

c. The AIOTF may retrieve information related to the requested UE from AMF, including its location, connection status and reachability.

6. The AIOTF, based on the information collected in step 5, validates whether the requested UE ID provided in the AF request can serve as an intermediate node.

7. If the requested UE is not operational and other "I-nodes allowed" flag was not set in the AF request, AIOTF sends AIOT Response with the failure reason to the AF, and the subsequent steps are skipped.

8. If the validation of the requested I-node fails and the 'other I-nodes allowed' flag was set in the AF request, the AIOTF may select a different list of UEs for the requested operation than the UE requested by the AF. This can be achieved by performing the step 5 in the figure 6.11.2.2-1 with the location set to the location information of the requested UE retrieved from AMF in step 5c.

9. The AIoTF requests the serving AMF to initiate the communication with the AIoT devices, which includes the target AIoT device IDs, and the selected I-node IDs.

10. The AMF forwards the AIOT read request to gNB along with the target AIOT device IDs and the selected I-node IDs.

11. The gNB performs additional validation to assess if the received I-nodes are optimal for serving the AIoT devices, considering its local conditions such as response time, received signal strength, etc. Subsequently, the gNB makes the final selection on the best I-node. It is also possible that the gNB does not select any of the requested I-nodes if local conditions are not satisfied.

12. The gNB may respond to the AIOTF via AMF with the final list of selected I-nodes.

### 6.11.3 Impacts on services, entities and interfaces

Impacts on existing entities:

NEF:

- Supports exposing a new API to AF for AIoT services.

UDM:

- Supports validating if a UE is authorized to act as an I-node.

AMF:

- Supports forwarding the AIOTF requests to gNB.

gNB:

- Supports handling new AIoT related services.

- Supports making the final selection of the I-node.

UE (I-node):

- Supports indicating its capability to support AIoT services during UE registration.

- Supports communicating with AIoT devices.

New NF:

- AIOTF:

- This can be a standalone NF or combined with NEF.

- Supports necessary network information for specific UEs or specific location from multiple NFs (e.g., AMF, UDM, NWDAF)

- Supports selecting or validating I-nodes.

- Supports forwarding the AF requests to AMF.

## 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 SA WG3 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.

## 6.13 Solution #13: Multi-level Device ID management

### 6.13.1 Description

When it comes to Ambient IoT Device ID Management, it is likely that different Device ID formats are expected depending on the procedures to be followed between Ambient IoT Device, Reader, Controller and Application Function.

On highest level, a Permanent ID is expected to enable uniquely identifying Ambient IoT Device by the 3GPP system. Such ID can entail MNO ID, Enterprise (Owner) ID, Instance ID (see solution #2 in TR 23.700-13).

However, such long Permanent ID can not be conveyed conveniently on all AS level procedures (e.g. between Ambient IoT Device and Reader) or non-AS level procedures (e.g. between Reader and Controller) due to large overhead or security issues.

As a result, it is expected that the Permanent ID of the Ambient IoT Device to be mapped to other temporary IDs across different entities / procedures.

This solution assumes the same principles on temporary ID assignment, mapping and interpretation is applicable to Ambient IoT Device, Reader, Controller irrespective of topology types.

### 6.13.2 Procedures

At least, two levels of temporary IDs are proposed:

* Long temporary ID: A long temporary Device ID to be used between the Controller and the Reader for command procedures (similar to paging) for certain Ambient IoT Device(s).

- A set of long temporary IDs can be assigned and pre-provisioned by the Controller to the Reader.

- The Controller maintains the mapping between long temporary ID and unique Ambient IoT Device identifier (e.g. based on the Permanent ID) per Device based on notification from the Reader.

- Only one Reader maintains the mapping of long temporary ID to short temporary ID per Ambient IoT Device.

- If CN paging fails, the Controller will inquire other Readers. The Controller pages the Ambient IoT Device using the device’s permanent (unique) ID at the last known Reader. On successful paging response / notification from one of the Readers (incl. the mapping of long temporary ID for paged Ambient IoT Device), the Controller will accordingly update the mapping between long temporary ID and unique Ambient IoT Device identifier.

NOTE 1: Long temporary ID does not need to be exposed to the Ambient IoT Device.

* Short temporary ID: A short temporary Device ID to be used between the Reader and Ambient IoT Device for exchanging inventory request/ responses or command (request)/ responses.

- The short temporary Device ID can be assigned and provisioned by the Reader to the Ambient IoT Device for message exchanges between the Reader and the Ambient IoT Device.

- The Reader maintains mapping between long temporary ID and short temporary ID per Ambient IoT Device.

- The Reader notifies the Controller on mapping of long temporary ID per ambient IoT Device (e.g. based on the Permanent ID).

NOTE 2: The exact format and further details of short temporary ID is in remit of RAN WGs.

NOTE 3: The temporary IDs can be reassigned (when needed) to limit the pool size of temporary IDs. However, the temporary IDs must be locally unique in the reader (for short temporary IDs) and in the Controller (for long temporary IDs).

Editor’s note: Validity time per temporary ID (either long or short) and if there is correlation between those two is FFS.

Editor’s note: It is FFS if short temporary ID is security protected.

### 6.13.3 Impacts on services, entities and interfaces

Controller:

- Assign and pre-provision a set of long temporary IDs per Reader

- Use long temporary ID as part of command procedures towards the Reader(s) for certain Ambient IoT Devices.

- Maintain the mapping between long temporary ID and unique Ambient IoT Device identifier (e.g. based on the Permanent ID) based on the notification from the Reader.

Reader:

- Assign and provision short temporary ID per Ambient IoT Device

- Map and Maintain mapping of the long temporary ID to short temporary ID per Ambient IoT Device

- Notify the Controller on mapping of long temporary ID per Ambient IoT Device (e.g. based on the Permanent ID)

Ambient IoT Device:

- Can interpret and respond to its assigned short temporary ID towards the Reader

## 6.14 Solution #14: AIoT Device ID with consideration on credential holder, service provider and mobile network

### 6.14.1 Description

This solution addresses the KI#2 and the aspect about how to identify Ambient IoT Device and how to format the identifier.

In this solution, the following terms have been used:

- AIoT Device ID: the identifier used to identify the AIoT Device;

- Serving network: PLMN network which includes the Reader and the radio/core network;

- Credential holder: This domain holds the credential associated with the AIoT Device ID;

- Service provider: This domain holds the application function for Inventory and/or Command.

The following stakeholders have been considered:

- Case 1: AIoT Device ID and its associated credential are managed by network (PLMN network operator):

- Case 1.1: AIoT Device ID and its associated credential are managed by the serving network (PLMN network operator). Service provider can belong to the same serving network (PLMN network operator) or 3rd party.

- Case 1.2: AIoT Device ID and its associated credential are managed by one network (PLMN network operator); the Credential holder is another PLMN network which is different from the serving network. Service provider may belong to the same serving PLMN network, or Service provider may belong to Credential holder associated to the PLMN network or 3rd party. In this case, the serving network and the credential holder has the "roaming like agreement" to ensure that the AIoT Device ID can be e.g. verified or authenticated.

- Case 2: AIoT Device ID and its associated credential are managed by the 3rd party:

- Case 2.1: AIoT Device ID and its associated credential are managed by service provider (3rd party); the serving network can be PLMN network. In this case, the Credential holder associated with AIoT Device ID is the service provider.

- Case 2.2: AIoT Device ID and its associated credential are managed by a 3rd party other than the service provider (3rd party). In this case, the serving network can be a PLMN network.

Editor’ note: It is FFS how to consider AIoT Device ID managed in the SNPN network.

In the case 1, since the AIoT Device ID and its associated credential are managed by the network (PLMN network operator), then AIoT Device ID has the information to identify the network. The format can be designed as shown in the figure 6.14.1-1. AIoT Device Identification Number is required to be unique in the PLMN network.



Figure 6.14.1-1 AIoT Device ID structure for case 1

In the case 1, the AIoT Device ID can also be in NAI like format <username> @ operator where the <username> part is assigned by the operator and the operator info can be used to identify the operator. In this format, the <username> part is required to be unique @operator.

NOTE: NAI like format does not mean it to be in the format of string.

In the case 2, since the AIoT Device ID and its associated credential are managed by 3rd party (service provider or e.g.AIoT Device manufacturer), then the AIoT Device ID has the information to identify the 3rd party (service provider or other 3rd party e.g.AIoT Device manufacturer). The format can be NAI like format<username> @ 3rd party (SP or and other 3rd party e.g. AIoT Device manufacturer). The username part is assigned by the 3rd party.

### 6.14.2 Procedures

This clause is to describe the high-level procedure including configuration and provisioning for 2 cases as specified in clause 6.14.1. Other details how to utilize the AIoT Device ID are specified in other solutions.

**Case 1**



Figure 6.14.2-1 High-level procedure for case 1

1. If the AF is in the 3rd party, then the 3rd party and the PLMN network have the service level agreement to ensure that exposure of AIoT Device ID is also secure.

2. The AIoT Device is provisioned with AIoT Device ID and associated credentials.

3. The AF performs the Inventory or Command with full or partial AIoT Device IDs to the PLMN network. The partial AIoT Device ID is some part of full AIoT Device ID. The full AIoT Device ID is <username> @ operator or full information as shown in figure 6.14.1-1.

Editor’ note: It is FFS what is the criteria to use the partial AIoT Device ID.

4. The PLMN network performs the Inventory or Command with full or partial AIoT Device IDs as in step 3 to AIoT Devices.

5. The involved AIoT Devices responds with the AIoT Device IDs together with the Inventory Response or the Command Response to the PLMN network. In this step, the PLMN network can perform the Authentication procedure or the AIoT Device ID verification procedure to check the AIoT Device valid or not.

Editor's note: The verification of AIoT Device ID and authentication requires coordination with SA3.

6. The PLMN network exposes the AIoT Device IDs to the AF.

**Case 2**



Figure 6.14.2-2 High-level procedure for case 2

1. The Credential holder and the service provider may be the same. The credential holder domain and the PLMN network have the service level agreement to ensure that the AIoT Device ID can be e.g.verified or authenticated.

2. The AIoT Device is provisioned with AIoT Device ID and associated credentials by the credential holder (service provider and other 3rd party e.g. AIoT Device manufacturer).

3. The AF performs the Inventory or Command with full or partial AIoT Device IDs to the PLMN network. The partial AIoT Device ID is some part of full AIoT Device ID. The full AIoT Device ID is <username> @ 3rd party.

4. The PLMN network performs the Inventory or Command with full or partial AIoT Device IDs as in step 3 to AIoT Devices.

5. The involved AIoT Devices responds with the AIoT Device IDs together with the Inventory Response or the Command Response to the PLMN network. In this step, the PLMN network can perform the Authentication procedure or the AIoT Device ID verification procedure with the involvement of credential holder (service provider and other 3rd party e.g. AIoT Device manufacturer) to check the AIoT Device valid or not. In this step, if the service provider is not the credential holder, then it is not involved in this step.

Editor's note: The verification of AIoT Device ID and authentication requires coordination with SA3.

6. The valid AIoT Device IDs are reported to the AF.

### 6.14.3 Impacts on services, entities and interfaces

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

## 6.15 Solution #15: Ambient IoT Device States

### 6.15.1 Description

#### 6.15.1.1 Overview

This solution addresses KI#2, KI#3 and proposes new states and sub-states for AIoT devices that may assist the AIoT services the AIoT device supports in any particular moment. In particular, the solution consists of the following aspects:

- A new set of states or mode of operations are defined for the AIoT device, which can be transitions to/from based on network requests, where these requests may come from the AF.

- A new service exposure is proposed that enables the AF to trigger a change in the AIoT device state (or mode of operation). This may also be performed by the network due to local configuration.

- The network and AIoT device can confirm the result of the state change (or change in mode of operation), or provide a report on the current state the AIoT device is currently in.

In this solution, an AIoT device state may also refer to an AIoT device mode of operation and/or to a service operation that the AIoT device can take while being in such state. As such the term state is not to be considered as a restriction that binds an AIoT device to a particular state but rather as an example of how the AIoT device may perform or behave in certain modes or conditions or based on service operations or expectations.

Note that an AIoT device may also be referred to as a UE, or an AIoT device may be considered a special type or category of a UE. A UE may have at least AIoT capabilities, or an AIoT device can be a UE with restricted capabilities.

Clause 6.15.1.2 describes new AIoT device states proposed by this solution and clause 6.15.2 describes a procedure to toggle the state of an AIoT device.

#### 6.15.1.2 New AIoT Device States

AIoT device states can be useful for the application and/or the network to be aware of which AIoT devices are already operating and which function they may be performing, which may in turn assist in their management and monitoring. As an example, the reliability of inventory taking results would be higher when all the AIoT devices that are meant to report identifiers, location, etc. are in a state validated by the network. Furthermore, an appropriate sub-state supporting event-based reporting allows an AIoT device to know how to behave after the event is detected, i.e. whether information regarding certain event should e.g. be reported, stored or ignored.

An AIoT device that has not yet been registered with the network may be in an INVALIDATED state. In this state, the AIoT device needs to be validated e.g. by going through authentication or other security procedures, or by its identity being validated. The AIoT device may also be validated as part of the registration process of the device with the network.

After a successful security and/or validation procedure, the AIoT device may enter a new VALIDATED state, where this is the main state of operation of this device.

Moreover, the AIoT device may operate on (or switch to) any of the following sub-states:

- REPORT-ONLY (or READ-ONLY): in this sub-state the AIoT device is only supposed (or allowed) to report data, or read data that has been collected and/or stored, and report the data.

- In this sub-state the AIoT device may report data either due to the AIoT device needing to report data e.g. periodically, or based on a solicitation (or command, trigger, and/or indication, etc.) from the network. This data reporting may not necessarily be due to a threshold being crossed (e.g. the data reporting may not necessarily be due to occurrence of an event). - RECEIVE-ONLY (or WRITE-ONLY): in this sub-state, the AIoT device may only receive data and/or commands from the network, and/or from an application function (AF) via the network, but this AIoT device does not report any data itself. Additionally, the AIoT device may be permitted to store this received data. The AIoT device may acknowledge the receipt of the data and/or command but may not send data. As an example, the AIoT device may toggle to a different sub-state, or stay in the same sub-state after receiving the data.

Editor’s Note: Whether separate dedicated REPORT/READ-ONLY and RECEIVE/WRITE-ONLY states are required is FFS.

Editor’s Note: Whether REPORT/READ-ONLY state permits data and/or service requests being received in the device is FFS.

- RECEIVE-and/or-EVENT-REPORT: in this sub-state the AIoT device only receives data and/or commands but can only report if particular events and/or conditions have occurred. For example, the event may be that a certain threshold has been crossed in relation to a parameter that has been sensed or monitored. In one example, upon the observed parameter exceeding a pre-configured threshold, the AIoT device enters or change sub-state to EVENT-REPORT in order to report the occurrence of this event to the network and/or the AF.

- In this sub-state, the AIoT device may not report even if solicited to do so as long as the event in question has not been detected. This differentiates this sub-state from the READ-ONLY or REPORT-ONLY sub-states.

Any of the functions above can be combined into one sub-state as well. For example, the WRITE-ONLY behavior may be part of the RECEIVE-ONLY sub-state.

Editor’s Note: The name of the above states/sub-states and whether additional states/sub-states incl. energy-related device states/sub-states can be defined is FFS.

Editor’s Note: Further details on how the above states may assist the service operations of AIoT devices is FFS.

The network may be configured to inform the AIoT device which state to start with, where this may be based on local policies or based on subscription information. As such, after validation of the AIoT device, the network may send a message, which may be part of the validation process or the registration process, to inform the AIoT device which state the AIoT device should start operating in. Alternatively, the AIoT device may indicate the desired state, and the network may verify whether the UE can operate in that state or not.

Editor’s Note: Whether and how this solution can be applied to a group of AIoT devices is FFS.

### 6.15.2 Procedure for State Toggling in AIoT Devices

An AIoT device may operate in any of the states described in clause 6.15.1.2. This clause proposes a method by which the network can toggle the AIoT device state by issuing a command such that the AIoT device will transition from one state to another. Toggling the state of an AIoT device may be useful e.g. after the AIoT device has been validated by the network for the AIoT device to know how it should respond to an inventory or read/write command. For example, the AIoT may reject or ignore such request if it is in INVALIDATED state described in clause 6.15.1.

This proposal is based on an interaction between an AF and the network, but it could also be locally based on policies of the network. The AF for example can have preference for a device to operate in a particular state only based on the usage of the device.

The main proposal in this clause is that the network should inform the AIoT device to change its expected behavior or set of functions, where each set of functions or expected behavior may correspond to a well-known action or behavior. A network entity (e.g. AMF) subscribes to the UDM for getting events related to a requirement to toggle an AIoT device state. NAS related signalling is supported, which could be a specific version of the NAS protocol for AIoT devices.

The dynamicity of the state toggling requests can be adjusted by the AF according to criteria such as minimization of complexity, energy consumption, etc.



Figure 6.15.2-1: Procedure to support toggling of states in an AIoT device

The procedure in Figure 6.15.2-1 to support toggling of states in an AIoT device is described step by step below.

1. The AF discovers the capability of the NEF exposure service, in particular the service to toggle the AIoT device state.

2. The AF provides a request to the NEF to toggle the AIoT device’s state. The AF identifies an AIoT device or group of AIoT devices in the request. The request also provides a clear indication that what is needed is to toggle an AIoT device(s)’s state(s) and as such the target state(s) is/are indicated. The current AIoT device(s)’s state(s) may also be indicated if necessary.

NOTE 1: A single AIoT device will be assumed in this solution hereafter but the solution can still apply to a group of AIoT devices.

3. The NEF communicates the request to toggle the AIoT device state with the UDM in order to verify if the AF is allowed to place such a request. The NEF may indicate the details of the request to toggle the AIoT device state to a target state, e.g. target state and/or current state. The NEF may also provide the identity of the AF.

4. The UDM verifies if the request can be granted based e.g. on the AF identity, the type of the request, etc. The UDM may indicate if the request is not authorized, or if the request can be authorized based on the above criteria.

5. The UDM determines which entity is responsible for this request, e.g. AMF, and communicates with such responsible entity to provide the request to toggle an AIoT device state indicating the target state to use.

Editor’s Note: Whether the AMF and/or other new or existing entities are responsible for this request is FFS.

Editor’s Note: It is FFS whether the AMF or any other 5GC NF stores information related to AIoT devices states.

6. The AMF sends a NAS message to the AIoT device indicating the new state the AIoT device should transition to. Alternatively the request may be to report the current state of the AIoT device.

Editor’s Note: Whether a protocol different from NAS may be used to indicate the new state to the AIoT device is FFS.

7. The AIoT device reports the result of the operation e.g. indicating if any state transition has been performed or reporting the current state of the AIoT device.

7a. The AIoT device transitions into a new state based on the request received from the network. This step assumes that the AIoT device has successfully toggled its state or that it can successfully do so. Otherwise if this is not possible then the AIoT device does not change its state.

NOTE 2: Step 7a may occur before the AIoT device reports the result of the operation to the network in step 7.

8. The responsible entity in step 5 (e.g. AMF) sends the result of the request to the source NF i.e. the UDM. The result may be that the AIoT device has changed its state or not, and the result may contain the AIoT device’s current state (which may be a new state e.g. in the case that the AIoT device has changed its state, or any other state such as the state that the AIoT device is in and that may not have changed based on the request from the network).

8a. The responsible entity in step 5 (e.g. AMF) updates the AIoT device’s state or context to reflect the new AIoT device state, based on the operation or result indicated by the AIoT device. If the operation or result is successful, then the responsible entity in step 5 (e.g. AMF) can update the AIoT device’s state, otherwise the AIoT device state is not updated and optionally a “failure to update” indication may be stored.

9. The UDM indicates the result of the request to update a AIoT device state (or to report the current state of the AIoT device) to the NEF. This may be based on the result received from the responsible entity in step 5 (e.g. AMF).

10. The NEF indicates the result of the operation e.g. the result to toggle the AIoT device state or to report the current AIoT device state.

### 6.15.3 Impacts on services, entities and interfaces

Editor’s Note: Impacts are FFS.

## 6.16 Solution #16: AIoT Registration/Onboarding

### 6.16.1 Description

This solution address the part of KI#2 related to the AIoT device registration/onboarding. The first bullet and NOTE 1 in solution#1 clause 6.1.2 mention the onboarding and parameter provisioning. This solution provides a procedure to achieve this.

The relation between this solution and solution 1, is that this solution will provide means to securely authenticate the AIoT device and provision the AIoT with necessary parameters to control the temporary ID as described in solution 1 i.e., an efficient way to generate new temporary ID and to enable AIoT device privacy protection. The proposed onboarding procedure requires minimum three messages to be sent over the radio interface, but the following Inventory and command procedures can be achieved with only two messages (one DL trigger + one UL) and fulfil the SA1 requirement in TS 22.369 [2] in clause 5.2.6.

*The 5G system shall be able to provide a mechanism to protect the privacy of information (e.g., location and identity) exchanged during communication between an Ambient IoT device and the 5G network or an Ambient IoT capable UE.*

NOTE: The actual number of physical messages sent over the radio interface between AIoT device and Reader depends on the RAN design. The numbers used above should be seen as the number of logical messages between the AIoT device and Reader.

As the CN NF would get the information of all AIoT devices that the CN NF performed this registration procedure with, it can also be seen as an initial Inventory collection by the network. This Inventory information can be exposed to an AF subscribing to such exposure service.

The solution is based on the following assumptions:

- The AIoT device is not capable to initiate the registration procedure. The Network will trigger AIoT devices to register.

- The AIoT reader (UE or Base station) periodically or on-demand broadcasts a message, Registration poll message, that triggers nearby unregistered AIoT device(s) to respond. The Registration poll message is assumed to be non-AIoT device specific to allow all unregistered AIoT device(s) to respond in an area.

- An AIoT device does not respond to the Registration poll message if it is already registered in the network or the PLMN is not allowed.

Editor’s note: Whether a registered AIoT device would responds to a Registration poll message to perform e.g. periodic registration is FFS.

- The AIoT device responds with a Registration Request that includes e.g., device owner ID and concealed device ID. This will allow the CN NF to retrieve further information to proceed with the registration/onboarding of the AIoT device. If the CN NF was not able to retrieve the required information or the AIoT device was not possible to authenticate and authorize, the AIoT device will be rejected to register in the network and shall refrain from trying to register again in this network.

- During the registration procedure the CN NF will provision the AIoT device with e.g., security parameters, initial TempID or parameters to derive the initial Temp ID i.e., parameters for the Temp ID generation algorithm as discussed in clause 6.1.

- An AIoT device has two states: Unregistered or Registered. The AIoT device will remain in Unregistered state until the AIoT device receives the Registration Accept message.

### 6.16.2 Procedures

CN NF is used to name the network function that performs the necessary task to register/onboard an AIoT device to the network. The CN NF will be defined together with the system architecture design to support the Ambient IoT in 5GC.



Figure 6.16.2-1: Registration/onbording procedure for an AIoT device.

0. It is assumed that the AIoT device is pre-provisioned by the device owner with information to be used when register/onboarding to a network. The information includes a device unique identifier (unique at owner level, not necessary globally unique), device owner ID and security IE.

Editor’s Note: Whether or not an AIoT device checks the network ID to a list of preferred network IDs stored in the device is FFS

It is assumed that the device owner and the MNO has an SLA. A device owner AF may have provisioned the network with information needed to onboard an AIoT device(s) or a URL or FQDN to establishing IP connection to an AF that holds the device unique onboarding information.

1. The AIoT reader (UE or base station) broadcasts a Registration poll message that includes e.g. the PLMN ID or NID. The broadcast can either be an immediate broadcast triggered by CN NF or a scheduled/periodic broadcast configured by the CN NF.

Editor’s Note: The format of the Registration poll message needs to be defined in cooperation with RAN WG.

2. An AIoT device that is not registered in the network responds with a Registration Request (device owner ID, concealed device ID). The Reader forwards the Registration request message to the CN NF.

Editor’s Note: How the concealed device unique ID is created will be defined by SA3.

Editor’s Note: Whether or not an AIoT device checks the network ID to a list of preferred network IDs stored in the device is FFS.

3. The CN NF may hold AIoT device owner information or can retrieve AIoT device owner information from the UDM/UDR using the received device owner ID. In case the AF has provisioned the network with the device unique information needed to onboard the AIoT device, then step 4 can be skipped.

4. The CN NF uses the retrieved AIoT device owner information to establish a secure IP connection with the AF to retrieve the device unique onboarding information by providing the concealed device ID to the AF. The AF must be able to un-conceal the device ID and verify that the device ID is part of the owner’s inventory list. The AF provides the CN NF with authentication/authorization result and device unique information needed to onboard the AIoT device e.g., device security information.

5. In case the AF have provisioned the network with device unique onboarding information in step 0, then the CN NF uses the retrieved information from UDM/UDR to authenticate and authorize the AIoT device.

6. The CN NF sends a Registration response (Accept/Reject, security parameters). The AIoT device uses the security parameters together with the pre-provisioned security IE to e.g., derive an initial Temp ID as proposed in solution 1. Additional AIoT configuration can be provision at this step.

### 6.16.3 Impacts on services, entities and interfaces

Impacts on existing entities:

CN NF:

- Configure/trigger the Reader to broadcast Registration poll message.

- Retrieve device owner information and device unique onboarding information.

- Accept or reject the AIoT device registration/onboarding request.

AIoT device:

- Receive a Registration poll message.

- Transmit a Registration Request message to the Reader.

- Receive the Registration accept message with configuration parameters.

- Manage state transition between Unregistered and Registered.

AIoT Reader (UE or Base station):

- Broadcast Registration poll (on-demand or periodically configured).

- Transparently forward any messages between the AIoT device and the CN NF.

UDM/UDR

- Data management of device owner information.

- Be provisioned with device owner information.

## 6.17 Solution #17: Enable Ambient IoT Management within 5GC to support AIoT services

### 6.17.1 Description

#### 6.17.1.1 General

This solution addresses the key issues in terms of architecture enhancements, Ambient IoT (AIoT) Device management and AIoT services, i.e., for KI#1, KI#2 and KI#3.

#### 6.17.1.2 Architecture Principles

This solution proposes to introduce enhancements in the 5GS to support AIoT Device management and AIoT services. In particular,

- AIoT specific NAS, to support transfer of AIoT data (AIoT Device Operation commands and responses) between AIoT Device and 5GC directly via the gNB.

- Ambient IoT Management Function (AIoTMF), responsible for the logic for handling of AIoT services including:

- execute the AIoT service request (e.g., inventory, read) in the network and handle any corresponding AIoT specific NAS messages,

- support inventory and message routing for AIoT Devices,

- authorize the AIoT service request,

- perform validation of the AIoT Device Identifier (ID) and secure AIoT Device operations if needed,

- collect AIoT data and aggregate the reporting,

- collect charging information if required by SA5.

- UDM enhancements to manage subscription-like information for AIoT Devices and service control information for 3rd party application:

- An AIoT Device ID is allocated to each AIoT device that has subscription-like information provisioned in the UDM. The AIoT Device ID shall be unique within a mobile network, and it is used to locate the subscription-like information. The format of the AIoT Device ID will be defined by other solutions.

- The subscription-like information for an AIoT Device is different from the UE subscription data. The subscription-like information contains: AIoT Device ID, security materials, and device status information e.g.last serving node, whether the AIoT Device is disabled, etc.

- As part of a provisioning process for an AIoT Device, the AIoT Device is provided with its AIoT Device ID, security materials and security settings which control what operations on which memory regions require what levels of security to be applied.

- The service control information is used to authorize the AF’s device operation request. The service control information, based on service agreements between the network operator and the 3rd party AF, may contain: AF ID, allowed service area, allowed service operations, allowed AIoT Device ID information etc.

- NEF enhancements to expose the 5GS AIoT capability so as to allow 3rd party AF to consume the AIoT services.

Figure 6.17.1.2-1 illustrates the enhancements to the 5GC to support AIoT Device management and AIoT services for topology 1.



Figure 6.17.1.2-1: 5GC enhancements to support Ambient IoT

Editor's Note: It is FFS whether AMF is needed

NOTE: From AIoT Device point of view, the interfaces with the network are the same for both Topology 1 Topology 2.

#### 6.17.1.3 Function Principles

**Inventory:** collect the AIoT Device ID(s) of all or a subset of AIoT Devices discovered and selected with MASK.

**AIoT Service:** the network capability that utilizes the NEF exposure capability towards AF and utilises the AIoT Device Operations towards AIoT Device to support AIoT use cases.

**AIoT Device Operation:** the operations the network supports to communicate with AIoT Device e.g., inventory, read, write, disable.

**MASK:** a full or partial AIoT Device ID, which will be broadcasted by a reader in order to select a specific group of AIoT Devices to perform random access and report their Device IDs to the network. The AIoT Device whose Device ID matches the MASK will perform random access to report the Device ID. This MASK can also reflect the information fully or partially of a 3rd Party-defined Identifier as described in step 3 and step 5 of Figure 6.17.2.2-1.

**Task ID:** an identifier generated by 5GC which is used to identify the AIoT Service requested by a 3rd party/AF. To deliver the information between AF and an AIoT Device over 5GS, the 5GC uses the Task ID to maintain the association within the 5GC for a specific AF’s AIoT service request from the time it accepts the AF’s AIoT service request to the time the AF’s AIoT service request is completed.

The 5GS shall support AIoT specific NAS to deliver the UL or DL data between AIoT Device and 5GC. The UL data includes the AIoT Device ID, Results of the Commands, security information, and Indication of cached data etc. The DL data includes the Commands and security information etc. There is a AIoT-NAS connection between AIoT Device and 5GC, and this AIoT-NAS connection is per device level. The AIoT NAS message is transferred over AIoT-NAS connection between AIoT Device and 5GC.

NOTE 1: AIoT Devices have reduced functionality compared to other types of UE (e.g., NR, eMTC or NB-IoT). An AIoT Device is more akin to a memory device (for example a flash memory card) that utilize basic memory comparison operation (match a bit sequence (e.g. the MASK) against memory location Y for length Z) to support identification, and then further operations for inventory, reading and writing data.

The physical memory of the AIoT Device can be logically viewed as containing multiple different types of information, e.g., 3GPP Information and Application Information: 1) The 3GPP Information is information that is known to and used by the 3GPP system. Examples of 3GPP Information include AIoT Device ID, Security Materials etc. 2) The Application Information is information that depends upon the application to use. Examples of use of the Application Information include the device having a fixed application defined memory format, where certain locations in the memory are known to contain information read/written by the application, sensor reading(s) or it can be used for more complex message passing techniques, e.g., being used as a mailbox. The contents and use of the Application Information is not expected to be defined by 3GPP, however 3GPP needs to define the operation primitives that allow reading, writing etc of the memory without detailed knowledge of its contents. The mapping of information / fields and their contents into physical memory is to be defined by Stage 3.

The AMF/AIoTMF and AIoT Device shall support to store a temporarily device context. The temporarily device context is kept in the AIoT Device and AMF/AIoTMF and is only used while energy is available to the AIoT Device, and it is used to record any information (e.g., security context) required for information transfer over AIoT-NAS connection (in particular for multiple-rounds of information exchange for example step 10~step 14 in figure 6.17.2.2-1) between the AIoT Device and AMF/AIoTMF. The temporarily device context helps avoid re-generation of e.g., security context each time a NAS message is transferred.

NOTE 2: As agreed by RAN, the AIoT Device memory can include two types of memory: 1) Non-Volatile Memory (NVM) such as EEPROM for permanently storing AIoT Device ID, etc. and 2) volatile memory (e.g. registers or RAM) for temporarily keeping any information required for its operation only while energy is available.

Editor's note: details for the temporary device context are FFS.

The 5GS shall support AIoT NGAP to control the behaviour of Reader, e.g., start of the inventory, continue of the inventory, end of the inventory. In addition, the AIoT NGAP provides transport of the AIoT NAS messages between Device and AMF/AIoTMF. The 5GS shall support AIoT-NGAP connection management for AIoT Service, this is used to transfer AIoT NAS message and AIoT inventory AIoT-NGAP message, e.g., reporting of RAN’s AIoT capability, requesting inventory for AIoT Device.

The high-level AIoT Protocol Stack is illustrated in the Figure 6.17.1.3-1.



Figure 6.17.1.3-1: AIoT Protocol Stack (Topology 1)

NOTE 3: AIoT AS and AIoT NGAP protocols will be defined by RAN, and it is assumed that the AIoT AS and AIoT NGAP message can transport NAS messages.

NOTE 4: The AIoT NAS needs to be lightweight to adhere to the nature of the AIoT Devices (e.g., ultra-low complexity power, cost and resource-constrained) while addressing e.g., confidentiality, integrity, etc. For example, Security header type, Message authentication code, and Sequence number are only needed if NAS security protection (e.g., Integrity protected, Integrity protected and ciphered) is required.

**AIoT Data:** This is used to transfer application specific AIoT data between AIoT Device and application. This layer is optional and supports customization and extension of advanced functions on top of the basic standard functions to meet diverse requirements in different scenarios.

**AIoT NAS**: This is used to indicate the operation commands, as well as transfer of the application specific AIoT data between AIoT Device and 5GC. AIoT NAS message includes e,g., Inventory Response, Read Service Request, Write Service Request, Disable Service Request, Command Service Accept. 5GC executes the AIoT service request from AF and generates the corresponding NAS messages, then triggers the reader(s) to perform inventory for AIoT Devices and transfer of the AIoT NAS messages between the AIoT Device and 5GC.

NOTE 5: It is assumed that the 5GC needs to indicate Reader RAN the different device operations to apply different handling for different AIoT Device operation commands e.g., Read or Write or Disable. And this will be further studied by RAN groups.

NEF exposure is used by the AF to invoke AIoT service (e.g., Inventory, Commands: Read, Write, Disable). Along with this AIoT service request, the AF is implicitly subscribed to receive notifications for its AIoT service request. At the same time, the NEF exposure can be used to deliver the UL or DL data for AIoT Devices between AF and 5GC. The DL data includes the Inventory Parameters and Command Parameters, and the UL data includes the Results of the Inventory and Command, Indication of cached data.

### 6.17.2 Procedures

#### 6.17.2.1 General

This clause provides end to end high-level information flow for support of AIoT service (Inventory, Command [Read/Write], Disable) over 5GS as specified in clause 6.17.2.2, as well as the NEF service operations as specified in clause 6.17.2.3.

#### 6.17.2.2 AIoT Service High-Level Information Flow



Figure 6.17.2.2-1: AIoT Service High-Level Information Flow

1. During the node-level AIoT-NGAP association establishment procedure, the RAN reports the RAN’s AIoT capability (Reader RAN ID, Indication of the RAN’s AIoT Capability, coverage area of the Reader RAN) to the AMF/AIoTMF.

2. Upon reception of the RAN’s AIoT capability, the AMF/AIoTMF aggregates the AIoT capabilities of all connected RANs and registers its AIoT capability into the NRF (AMF/AIoTMF ID, coverage area for AIoT service).

3. AF sends AIoT service operation request to NEF, carrying the AF ID, device information, and reporting control information.

The device information includes one or more of the following:

- device area information, indicates the requested area where the inventory service will be performed.

- device filter information: indicates complete or partial of 3rd Party-defined Identifier, and is used to compose the MASK used in step 5 to filter the Ambient IoT Devices to be inventoried.

The reporting control information indicates when and how to send the reports, e.g., immediate reporting of new result or progress, periodic reporting, one-time reporting at the end of the AIoT service procedure, and it can also indicate to report cached data along with the AIoT Device ID etc.

The AIoT service operation can be AIoT\_Inventory service operation or AIoT\_Command service operation or AIoT\_Disable service operation as specified in clause 6.17.2.3. If the AIoT service operation is AIoT\_Command service operation, the AIoT service operation additionally includes the AIoT Device operation command information, which indicates Read, or Write and command related parameters (e.g., memory location to start, length to read/write or data to write). If the AIoT service operation is AIoT\_Disable service operation, the AIoT service operation additionally includes the AIoT Device Disable operation command related parameters (e.g., signature and password).

4. NEF invokes NRF to discover and select the AMF/AIoTMF(s) using the AF requested device area information. The NRF determines the target AMF/AIoTMF(s) based on the AF requested device area information and the AIoT capability of the registered AIoTMF in step 2.

5. NEF sends the AIoT service operation request to each of the selected AMF/AIoTMF. The AMF/AIoTMF may obtain the service control information from UDM.

The AMF/AIoTMF performs the permission control of the AIoT service operation request based on the operator policy, service agreement between the AF and the operator, and information obtained from the UDM, e.g., based on service area which allows the AF to request the service operation, or subscribed service operation(s) that allows the AF to invoke. If not authorized, the AMF/AIoTMF rejects the AIoT service operation request with an appropriate cause code, and step 7 onwards are skipped. Once the AIoT service operation request is authorised, the AMF/AIoTMF generates a Task ID corresponding to this AF service operation request, as well as the associated device MASK information based on device information (received in step 3), information obtained from the UDM, and/or local configuration.

If the AIoT service operation is AIoT\_Disable service operation, the AMF/AIoTMF additionally determines the AIoT Devices that have subscription-like information in UDM and match with the device information (received in step 3). The AMF/AIoTMF performs validation of the signature provided by the AF, and if validated, it stores the password and sets the device status in UDM to "TO BE DISABLED" for the determined AIoT Devices. With this "TO BE DISABLED" indication, the 5GC won’t provide AIoT service to AF for those AIoT Device.

6. NEF sends the AIoT service operation response to the AF, containing the accept or reject result for the AIoT service operation request.

7. The AMF/AIoTMF selects the Ambient IoT capable RANs, taking the device information (e.g., AF requested device area information) and information obtained from the UDM (e.g., allowed service area) into account.

8. For each of the selected reader RAN, the AMF/AIoTMF sends the Inventory Start NGAP message (node-level AIoT NGAP message) with the device MASK information and the Task ID generated in step 5.

If the AMF/AIoTMF receives the AIoT\_Command or AIoT\_Disable service operation request, the Inventory Start NGAP message additionally includes the indication that transfer of AIoT NAS Command message subsequently.

If no “command indication” received, Reader RAN will continue to the next matched AIoT device and step 13 -step 16 are skipped.

If the AMF/AIoTMF receives indications to report cached data along with the Device ID, the Inventory Start NGAP message also includes the indication of data reporting.

9. Upon reception of the Inventory Start NGAP message, RAN/Reader executes inventory Task by triggering the Paging-like procedures with the device MASK information and indication of data reporting (if received in step 8) towards the AIoT devices.

10. If an AIoT device matches the device MASK information, the AIoT device performs random access like procedures to establish the AS connection with RAN.

11. The AIoT Device sends the truncated AIoT Device ID in AIoT Inventory Response NAS message. The truncated AIoT Device ID is a partial AIoT Device ID without MASK. The AIoT Inventory Response NAS message is encapsulated within the A-Uu message sent to Reader/RAN, and the RAN/Reader relays the AIoT Inventory Response NAS message over AIoT-NGAP message (Task ID, RAN NGAP ID, AIoT NAS) to AMF/AIoTMF.

If the AIoT Device has cached data, the AIoT Device also includes the Indication of the cached data in the AIoT Inventory Response NAS message, or if the AIoT Device receives the indication of data reporting in step 9, the AIoT Device includes the cached data in AIoT Inventory Response NAS message.

Based on the received indication that transfer of NAS Command message in step 8, the Reader RAN allocates the RAN NGAP ID and keeps the NGAP context for this selected AIoT Device.

12. The AMF/AIoTMF constructs the entire AIoT Device ID by adding the MASK information on the partial AIoT Device ID. The AMF/AIoTMF performs validation based on the device subscription-like information received from the UDM, including Device ID validation. The AMF/AIoTMF updates the device status for this AIoT Device in the UDM, e.g., last serving node.

If the device status indicates "TO BE DISABLED" for AIoT\_Inventory or AIoT\_Command service operation,

- In case of AIoT\_Inventory service operation, the AMF/AIoTMF records the AIoT Device ID and the serving node for this AIoT device. In a later time, the AMF/AIoTMF performs the step 7~16 to disable this AIoT Device.

- In case of AIoT\_Command service operation, the AMF/AIoTMF in step 13 proceeds as AIoT\_Disable service operation instead of AIoT\_Command service operation to disable this AIoT Device.

If the device status indicates "DISABLED", the AIoT Device ID of this AIoT Device is discarded and subsequent steps are not pursued for this AIoT Device.

13. [Conditional] If the AIoT service operation is AIoT\_Command or AIoT\_Disable service operation, the AMF/AIoTMF constructs the corresponding AIoT Command NAS messages (e.g., AIoT Read Service Request NAS message, AIoT Write Service Request NAS message, AIoT Disable Service Request NAS message), and the AIoT Device operation command related parameters as described in step 3 are payload of the AIoT Command NAS message.

The AMF/AIoTMF sends the AIoT Command NAS message to the AIoT Device. This AIoT Command NAS message is sent to RAN/Reader over AIoT- NGAP message (Task ID, RAN NGAP ID, CN NGAP ID, AIoT NAS), and then the AIoT Command NAS message is relayed by Reader RAN to the AIoT Device over A-Uu message.

14. [Conditional] If the AIoT Device receives the AIoT Command NAS message, the AIoT Device generates the results of the AIoT Device operation command and sends the AIoT Command Service Accept NAS message to AMF/AIoTMF. The results of the AIoT Device operation command are carried as payload of the AIoT Command Service Accept NAS message. The AIoT NAS message is sent to Reader RAN over A-Uu message and then the AIoT NAS message is relayed by Reader RAN to AMF/AIoTMF over AIoT-NGAP message (Task ID, RAN NGAP ID, CN NGAP ID, AIoT NAS).

If the AIoT Device receives the AIoT Disable Service Request NAS message, the AIoT Device needs to perform validation with the received password.

NOTE: Other security mechanism than the password based approach to support AIoT service needs coordination with SA3 WG.

15. [Conditional] If the AIoT service operation is AIoT\_Command or AIoT\_Disable service operation, and when the AMF/AIoTMF completes the device operation on the selected AIoT device, the AMF/AIoTMF sends the Inventory Continue NGAP message (Task ID, RAN NGAP ID, CN NGAP ID) to the RAN/Reader. Upon reception of this AIoT-NGAP message, the RAN/Reader releases the NGAP context for the current AIoT device and continues looking for next matched AIoT device.

16. [Conditional] If the AIoT service operation is AIoT\_Disable service operation, and when the Disable Operation is completed successfully for one AIoT device, the AMF/AIoTMF sets the device status of this AIoT device in UDM to " DISABLED". With this " DISABLED" indication, the 5GC won’t provide AIoT service to AF for this AIoT Device and the 5GC can delete the subscription-like information immediately or after a configured time period.

17. [Conditional] If the reporting control information matches (e.g., immediate reporting of new result or progress, periodic reporting), the AMF/AIoTMF reports the AIoT Device ID (s), results of the AIoT Device operation command and if available, the reported data or indication of cached data to NEF by sending the AIoT\_ Notify message (list of Device IDs, results of the AIoT Device operation command, reported AIoT data or indication of cached data). The NEF forwards the received information to AF by sending the AIoT\_ Notify message.

Reader RAN repeats steps 10~17 if there is a next matched AIoT Device.

18. The RAN/Reader sends the Inventory Complete NGAP message (Task ID) to AMF/AIoTMF in case of e.g., there is no further Ambient IoT Device performing random access, or AMF/AIoTMF proactively sends the Inventory Complete NGAP message (Task ID) to RAN/Reader in case of e.g., all target Ambient IoT Device(s) have been inventoried. The RAN Reader confirms the Task indicated by Task ID is completed.

19. The AMF/AIoTMF completes the Task for AIoT service operation request for each selected RAN/Reader. The AMF/AIoTMF reports the progress of the AIoT service operation request to the NEF by sending the AIoT\_ Notify message, the NEF informs the AF of the progress of the AIoT\_Inventory request by sending the AIoT\_Notify message.

If the reporting control information matches e.g., one-time reporting at the end of the AIoT service procedure, the AMF/AIoTMF can further aggregate the Device ID(s) and/or results of the AIoT Device operation command and reported AIoT data or indication of cached data. The AMF/AIoTMF further performs filtering and then includes into AIoT\_ Notify message the list of Device IDs, reported AIoT data or indication of cached data, results of the AIoT Device operation command etc.

#### 6.17.2.3 NEF AIoT Service

The NEF supports a new Nnef\_AIoT service with the operations described in table 6.17.2.3-1.

Table 6.17.2.3-1: AIoT Service provided by NEF

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| **Nnef\_AIoT\_Service** | Inventory | Request/Response | AF |
|  | Command | Request/Response | AF |
|  | Disable | Request/Response | AF |
|  | Notify | Subscribe/Notify | AF |

**Inventory Service Operation**: The inventory operations for the Nnef\_AIoT service allows the consumer to request to perform an inventory device operation for an AIoT device or a group of AIoT devices.

**Command Service Operation:** The command operations for the Nnef\_AIoT service allows the consumer to request to perform a read or write device operation for an AIoT device or a group of AIoT devices.

Editor's note: It is FFS whether differentiation of "Read" or "Write" AIoT device operations is needed. And if needed, whether to design separate AIoT service operations for "Read" or "Write" AIoT device operations, or to use an explicit parameter in AIoT\_Command service operation to differ "Read" or "Write" AIoT device operations.

**Disable Service Operation:** The disable operations for the Nnef\_AIoT service allows the consumer to request disabling RF transmission from an AIoT device or a group of AIoT devices. If the AIoT Device is disabled then the network may also discard any stored state for the AIoT Device and no further operations for that AIoT Device will succeed.

**Notify Service Operation:** The notify operations for the Nnef\_AIoT service allows the consumer to receive the status and results of the requested service operation.

### 6.17.3 Impacts on services, entities and interfaces

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

## 6.18 Solution #18: Solution for support of Ambient IoT services

### 6.18.1 Description

This solution resolves Key Issue #3 about the Support of Ambient IoT Services. 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 that is under the network control.

The third Ambient IoT AF triggers the Ambient IoT service toward ambient IoT devices via 5GS. In some Ambient IoT services, such as inventory, read, and others, one Ambient IoT service request from AF will cause numerous responses from ambient IoT devices, which may cause a severe signal storm in the 5GS. In order to mitigate the signal storm impact, we suggest that Base Station Reader supports response signal packet aggregation at the IP transportation level if Base Station Reader can’t look into the response packet content. If Base Station Reader can decode the response packets, Base Station Reader supports aggregation at the content level. At the same time, the AMF or new Ambient IoT NF supports content-level aggregation too to significantly reduce signal storm impact.

Besides, this solution aims to solve the issue of how the serving Base Station Reader or UE allows access from the different operators’ ambient IoT devices. The third ambient IoT AF has the information on the serving operator and the operators list of who provides ambient IoT devices in each location. The third ambient IoT AF includes EPC, an operator ID list, and location info in the service request toward the serving operator NEF. Based on SLA agreement between the third ambient IoT AF and serving operator, the NEF will check the operator ID list to allow it or not. If allowed, then serving operator NEF will forward the both EPC and operator ID list to Base Station Reader or UE. Base Station Reader or UE will utilize both EPC info and the operator ID list to identify the targeted ambient IoT devices in the service operations. Once the ambient IoT devices are matched by both EPC info and the Operator ID list (the device ID contains Operator ID info), they will respond to the request. Please note that if only EPC is matched, but operator ID is not matched, the ambient IoT device should not respond to the request. In this way, serving operator can control and allow the access from the different operators’ ambient IoT devices.

The principles related to Ambient IoT services are depicted below:

- The Ambient IoT device has a unique ambient device ID which consists of MNO operator ID, Company info, and instance ID. Device ID will not be exposed to the third Ambient IoT AF.

- Ambient device ID is stored in ambient IoT device.

- The third Ambient IoT AF will use EPC , location info and operator ID list to perform flexible Ambient IoT service. EPC is used to define a specific ambient IoT device or a group of ambient IoT devices. Operator ID list is used to allow access from the different operators’ ambient IoT devices.

- To mitigate signal storms in the 5GS, the UE, Base Station Reader, and AMF/New Ambient IoT NF can perform aggregation based on transaction ID.

- Both Leveraging existing AMF and Introducing new Ambient IoT NF apply to this solution.

### 6.18.2 Procedures

#### 6.18.2.1 Ambient IoT service --- Network initiated Ambient IoT service procedure

Figure 6.18.2.1-1: Network Initiated Ambient IoT service procedure.

AMF or New

Ambient IoT NF

10.Base Station Reader may aggregate the Ambient IoT Devices’ response info at the rough packet level or precise content level

5. Ambient IoT Service Request (Transaction ID, Service Type, TAC lists, Operator ID list, TID List, EPC info, Aggregation indication, time, periodical indication…)

7. Ambient IoT service request (Transaction ID, Service Type, Operator ID list, EPC info, TID List, Aggregation indication, time, periodical indication…)

9. Base Station Reader performs service operations with Ambient IoT Devices based on the Operator ID list and EPC or TID list info; Matched ambient IoT devices will respond with the device ID, TID, EPC info, and so on

devices based on User

ID lists

8. Base Station Reader decides targeted Ambient IoT devices based on both the Operator ID list and EPC info or TID info

6. Obtain targeted Base Station Reader based on TA lists;

Ambient AF

fd

UDM

NEF

Base Station Reader

UE

Ambient IoT

Devices

2. Ambient IoT Service Request (Transaction ID, Service Type, EPC info, location list, Operator ID list, TID List, Aggregation indication, time, periodical indication…)

1. Ambient IoT Device Activation and Registration Procedure

4. NEF communicates with UDM to obtain serving AMF or Serving new Ambient IoT NF lists based on TA lists ….

13. Ambient IoT service response (Transaction ID, aggregated Ambient IoT devices’ response Content…)

11. Ambient IoT service response (Transaction ID, response info)

14 Ambient IoT service response (Transaction ID， aggregated Ambient IoT devices response content…)

3. AF authentication and authorization/ Operator ID list check

12. Device ID checks and duplicated response records remove and aggregate the Ambient IoT Devices response info based on aggregation indication

1. Ambient IoT devices perform activation and registration procedures. Ambient IoT devices will have the EPC info and device ID, and UDM will have the Ambient IoT device profile info indexed by device ID after successful Ambient IoT devices activation and registration procedures. Besides, the device ID contains operator ID info, Company info, and instance ID. Ambient IoT device ID will not be exposed to the third AF, and it is used in Ambient IoT devices and 5GS as internal ambient IoT device identification for access, routing, and so on.

2. The third Ambient AF has the store location information and relevant AIoT serving operator info. The third Ambient AF launches an Ambient IoT service request towards NEF belonging to the AIoT serving operator. In the Ambient IoT service request, the third Ambient AF will provide Transaction ID, Service Type, EPC info, Location info, Operator ID list, Aggregation indication, time, periodical indication, and other parameters to NEF:

- Service Type: This information is used to define Ambient IoT service types, such as Inventory, Read, Write, and so on.

- EPC info: This information is used to define the targeted ambient IoT devices in the service from the products' perspective. it could be one specific ambient IoT device or a group of ambient IoT devices

- Operator ID list: This information is used to define the targeted ambient IoT devices in the service from the operator's perspective, supporting multiple operator ambient IoT device access. It could be one specific operator or a list of operators.

- TID list: The information can be used to define the targeted ambient IoT devices, such as in the write or read service command.

- Location info: This information is used to define locations where service happens.

- Aggregation indication: It is used to tell the 5GS how to handle the response messages -- aggregation response or not

- Time: when the service will be carried out exactly

- Periodical indication: the service operation will be executed periodically.

2. NEF will perform the below actions towards the third Ambient AF:

- Perform authentication to the third Ambient AF to decide whether it is allowed to access 5GS or not.

- Check the authorization to decide whether the third Ambient AF is allowed to perform certain Ambient IoT service operations or not.

- Check the authorization to see whether multiple Operators' ambient IoT device access is allowed or not.

- Converting location information to TA List information.

3. NEF will obtain serving AMF or serving New Ambient IoT NF based on TA lists

4. NEF forwards Ambient IoT service requests to serving AMFs or Serving New Ambient IoT NFs. Both leveraging existing AMF and introducing new ambient IoT NF can be applied to this solution.

5. AMF or New Ambient IoT NF determines the serving Base Station Readers based on TA lists. AMF or New Ambient IoT NF decides to perform aggregation operations in terms of aggregation indication.

6. AMF or New Ambient IoT NF forwards the Ambient IOT service request to the serving Base Station Readers.

7. Base Station Reader decides what kind of service operation to perform based on Service Type, and Base Station Reader decides to perform aggregation operations in terms of aggregation indication. Base Station Reader decides when to execute service operations based on time parameters, whether to perform periodical operations based on periodical indication and so on.

8. Base Station Reader performs service operations toward the serving ambient IoT devices. Both EPC info and the Operator ID list will be used in the service operation to identify the targeted ambient IoT devices. Once the ambient IoT devices are matched by both EPC info and the Operator ID list (the device ID contains Operator ID info), they will respond with the full device ID, TID, EPC info, and so on based on service operation type.

9. Base Station Reader will perform the response packet aggregation operation at the rough packetlevel based on transaction ID in terms of aggregation indication to mitigate signal amounts between Base Station Reader and 5GC if Base Station Reader can’t decode the response packets to look into the content. If Base Station Reader can decode the response packets to look into the content, Base Station Reader should perform the aggregation operation at the content level based on the transaction ID in terms of aggregation indication to further deduce signal amounts significantly between Base Station Reader and 5GC. Base Station Reader can decide the aggregation waiting time based on local configuration or AF indication.

10. Base Station Reader responds with an Ambient IoT service response message with parameters—transaction ID, Aggregated Inventory content, and so on—to AMF or the new Ambient IoT NF.

11. The AMF or new Ambient IoT NF will implement the Ambient IoT device check, remove duplicate Ambient IoT device records, and implement an aggregation operation at the content level based on the aggregation indication.

12. The AMF or new Ambient IoT NF continues to forward the response to NEF.

13. NEF will forward the response to the third Ambient AF.

Editor’s Note: This solution focuses on Topology 1. How to expand the solution to support Topology 2 is in FFS.

Editor’s Note: The security concern about how to access Ambient device is in FFS.

### 6.18.3 Impacts on services, entities, and interfaces

This solution impacts the following entities.

NEF：

- Capability to support the selection of the serving AMF or serving new Ambient IoT NF based on location information.

- Capability to aggregate the retrieved Ambient IoT devices' EPC contents based on transaction ID.

- Capability to support Ambient IoT service-related procedures.

- Capability to authentication and authorization to the third ambient IoT AF.

- Capability to support verification on operator ID list.

AMF or New Ambient IoT NF:

- Capability to support Ambient IoT service-related procedures.

UDM:

- Capability to manage the subscription information of Ambient IoT devices indexed by ambient device ID.

UE:

- Capability to support ambient IoT service procedures in terms of EPC and operator ID list

- Capability to aggregate the retrieved Ambient IoT devices' response at content level

- Capability to support Ambient IoT service-related procedures with 5GC.

Base Station Reader:

- Capability to support ambient IoT service procedures with Ambient IoT devices in terms of EPC and operator ID list.

- Capability to aggregate the Ambient IoT devices' response at IP transportation level or content level

- Capability to support Ambient IoT service-related procedures with 5GC.

## 6.19 Solution #19: AIoT communication for connectivity topology 1

### 6.19.1 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.*

- 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.*

### 6.19.2 Functional Description

This solution focuses on the Topology 1. It is proposed that the AIoT is a new radio access technology (RAT) type supported in the Base Station (BS). The BS nodes supporting the AIoT RAT establish N2' association with the 5GC (specifically with the AIoT function, AIoTF). The N2' association is independent of the N2 association for the communication via NR RAT or LTE RAT with the AMF.

This solution proposes that a new NF called Ambient AIoT function (AIoTF) is introduced. The AIoT application function or server (AIoT AF/AS) establishes an association with the AIoTF and transmits the AIoT data/information to the BS AIoT Reader via the AIoTF. The assumed architecture is shown in Figure 6.19.2-1.



**Figure 6.19.2-1: Assumed architecture for topology 1**

The AIoTF implements the following functionalities:

- Receive a request to establish an N2-like association (e.g. called N2' association) from an AIoT capable BS acting as “reader” for AIoT devices. The BS can indicate the AIoT radio coverage area, its location etc.

- Store the AIoT service parameters and configuring the BSs.

- Establishing an AIoT session with the AIoT AF/AS for transmission of AIoT data/signalling in a target transmission area.

- Selecting appropriate AIoT capable BS(s) for the transmission of AIoT data/signalling to the target transmission area.

- Receiving and transmitting AIoT data/signalling from/to the AIoT application server.

- Receiving and transmitting AIoT data/signalling from/to the BS acting as AIoT reader.

- Perform store-and-forward functionality for the AIoT data/signalling.

- To verify the identity of the AIoT device(s) and the security protection of the AIoT data/signalling.

- Creating charging data for the AIoT data/signalling and transmit the data to the CHF.

### 6.19.3 Procedures

#### 6.19.3.0 General

Two procedures are shown to explain the concept of this solution:

- the procedure for N2' association establishment for AIoT data/signalling transmission for connectivity topology 1; and

- the procedure for and AIoT service-based session establishment between the AIoTF and the AIoT AF/AS and AIoTF and the BS AIoT Reader via the N2' association.

#### 6.19.3.1 N2' association establishment

The Figure 6.19.3.1-1 describes the signalling flow of the N2-like (N2') association establishment between of AIoT capable BSs for reader functionality (called "BS AIoT Reader)" and the AIoTF.

The Figure 6.19.3.1-1 shows AIoTF1 and AIoTF2 to express the optional flexibility that a BS AIoT Reader can establish N2' associations to multiple AIoTFs.



**Figure 6.19.3.1-1: Signalling flow of the N2' association establishment between of AIoT capable BS node and AIoTF**

The detailed description of the steps is provided as follows:

1. The BS implements capability for AIoT transmission to AIoT devices (e.g BS AIoT Reader). The BS AIoT Reader stores various parameters for AIoT communication, e.g. power mode operation for AIoT, whether the BS AIoT is mobile or stationary, supported frequency bands for AIoT transmission, range of communication, etc. Each BS AIoT Reader is configured with an identifier, location information (e.g. GPS coordinates) and/or radio coverage area.

NOTE 1: The BS AIoT Reader is configured by the RAN OAM system.

The BS AIoT Reader can implement an AIoT client functionality which may receive and transmit 1) AIoT data/signalling from/to the AIoTF and 2) transmit and receive AioT data/signalling to/from the AIoT devices.

NOTE 2: The RAN architecture for AIoT is in the remit of the RAN WGs, e.g. whether the AIoT RAN includes one or more BS AIoT readers organized in hierarchical manner.

2. The BS AIoT Reader selects an AIoTF to register with. The BS AIoT Reader may be preconfigured (e.g. from the OAM system) with the AIoTF selection information. The BS AIoT Reader initiates the establishment of TNLA and N2-like association (e.g. called N2') with the AIoTFs.

The figure shows that the BS AIoT Reader establishes N2' associations and registers with the AIoTF1 and AIoTF2.

3a. and 3b. The AIoTF1 and AIoTF2 create its AIoT service area which is a combination of the AIoT radio coverage area received from the BS AIoT Readers.

4. The AIoTFs register with the NRF. For example, the AIoTFs use Nnrf\_NFManagement\_NFRegister service operation and indicate to the NRF the AIoTF type, the supported AIoT service IDs it is configured to serve (please refer to clause 6.19.3.2), the AIoT service area, AIoT capability (e.g. CP transmission or UP transmission) etc.

#### 6.19.3.2 AIoT session establishment between the AIoTF and the AIoT AF/AS and AIoTF and the BS AIoT Reader

The Figure 6.19.3.2-1 describes the signalling flow of the AIoT session establishment between the AIoTF and the AIoT AF/AS and between the AIoTF and the BS AIoT Reader via the N2' association. Such AIoT session is established for a particular AIoT service, e.g. inventory service or command/response service to AIoT devices associated with the AIoT service, and for a specific service area.

NOTE 1: In one example, the AIoT session can be used to allow the AIoT AF/AS to send a single request for AIoT service (e.g. read the AIoT sensors in a certain area), enable the AIoTF to create and send (e.g. periodically or a single request)the AIoT signalling to the AIoT devices in the target area, and the AIoTF reports the retrieved AIoT data to the AIoT AF/AS. In another example, if the AIoT AF/AS sends the AIoT data for each AIoT device, then the AIoT session is established to avoid the AIoTF selection in a target area for each AIoT data to a particular area.



**Figure 6.19.3.2-1: Signalling flow for AIoT session establishment between the AIoTF and the AIoT AF/AS** **and AIoTF and the BS AIoT Reader via the N2' association for a particular target area**

The detailed description of the steps is provided as follows:

1. The UDM/UDR stores AIoT device subscription data and (AIoT) application subscription data. The application subscription data contains the configuration information for the AIoT application (or also called AIoT service). The AIoT device subscription data can include individual device ID and corresponding credentials.

The whole step 2, including steps 2a, 2b, 2c, and 2d, describes a request to create (or update) an AIoT session between the AIoT AF/AS and the AIoTF for a particular target area.

2a. The NEF expose a new service to AFs offering the AIoT session establishment. Such service can be called Nnef\_IoTsession and can have the service operations Create, Update and Delete. The AIoT AF/AS uses this service and send a request including parameters like: external AIoT service/application ID, service type, target transmission area, application/service description parameters (e.g. service monitoring time, periodicity for monitoring, reporting, transmission time to device, UP/CP reporting, AIoT AS destination address, etc.).

The target transmission area is the area to which the to which AIoT data/signalling is to be transmitted. The target transmission area is mapped to one or more service areas of the AIoTFs.

2b. The NEF authenticates and authorizes the service request from the AIoT AF/AS.

2c. The NEF selects serving AIoTFs depending on 1) how the target transmission area (received in step 5a) maps to the AIoTF’s AIoT service areas and 2) what is the requested service type (e.g. inventory service or read/write service (also referred as command service)).

2d. The NEF forwards the request message for AIoT session establishment to the selected AIoTF. The AIoTF can expose a service like Naiotgw\_Session\_Create. The NEF uses the AIoT service/application ID corresponding to the external identifier from step 2a.

3. The AIoTF can retrieve from the UDM/UDR application subscription data by using the internal AIoT service/application ID as input parameter. The application subscription data can include credentials for network layer security to security protect (e.g. encryption and/or integrity protection) of the AIoT data/signalling transmitted to the AIoT device(s) belonging to the AIoT service ID.

4. The AIoTF creates a context for the AIoT service/application ID. The context may include the session service area, application/service description parameters, AIoT AS reporting address.

The session service area is the intersection of the target transmission area and the AIoTF-specific AIoT service area. If the target transmission area is smaller than the AIoT service area, the AIoTF uses the target transmission area as session service area. The AIoTF find the appropriate BS AIoT Reader(s) to which AIoT data/signalling is transmitted and which are part of the session service area. If the target transmission area is larger than the AIoT service area, then the AIoTF selects its whole AIoT service area as session service area.

5. The AIoTF sends a response to the AIoT AF/AS to acknowledge the AIoT session create/update request from step 2a. The response message can include the AIoT service/application ID, Session ID#1, session service area, etc.

Editor's Note: It is FFS upon which events the AIoT session between the AIoT AF/AS and the AIoTF can be modified or deleted.

The following steps 6a, 6b, 6c, 7 and 8 build a procedure for AIoT signalling transmission for the AIoT session. The AioT signalling to the AioT devices is created by the AioTF and the replies from the AioT devices are processed in the AIoTF. The AIoTF sends one or more reports to the AIoT AF/AS for the AIoT session.

6a. In one option, the AIoTF can create an AIoT signalling/data to be transmitted to the AIoT devices. In another option, the AIoTF can receive DL AIoT data to be transmitted from the AIoT-AS. The AIoTF uses a N2' procedure to carry the AIoT signalling/data to the BS AIoT Reader. The Downlink AIoT signalling transport message may include the target AIoT device ID, AIoT signalling, radio target area. The AIoT signalling may include an indication for inventory service to check the AIoT device ID and possibly type of good to which the AIoT device is attached.

NOTE 2: In one example, the identification of the type of good or product can be bound to the AIoT device identity as described in Annex A "Overview of the Electronic Product Code". In another example, a separate good or product identity ID, to which the AIoT device is attached, may be used, e.g. as described in GS1 organisation [11].

NOTE 3: The identification of the AIoT device and the applied security is not in the scope of this solution.

6b. The BS AIoT Reader transmits the AIoT signalling to the AIoT device(s). The AIoT device can backscatter the device ID and type of good to which the AIoT device is attached.

The AIoT device may verify the ID and security protection of the received DL AIoT signalling.

6c. The BS AIoT Reader receives the reply from the AIoT device (e.g. from the backscattered signals. The BS AIoT Reader creates a report transmits the report to the AIoTF.

7. The AIoTF processes the message received from the BS AIoT Reader. The AIoTF may verify the device ID and/or other parts of the AIoT signalling using AIoT device credentials retrieved from the UDM/UDR (e.g. as part of the AIoT device subscription data).

8. The AIoTF creates and transmits a notification message (which can be also a bulk message) to the AIoT AF/AS including the Session ID, AIoT service/application ID, AIoT signalling result like status of the device (e.g. type of good to which the device is attached, ID verification failed/succeeded), AIoT device location.

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

The following NFs and interfaces are impacted:

- AIoTF: a new NF with the functionality described in clause 6.19.2.

- BS AIoT Reader: 1) supporting AIoT capabilities to communication with the AIoT devices and 2) capabilities to select an AIoTF and to establish N2' association with the AIoTF.

- NEF: expose a new API for AIoT session creation.

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

## 6.20 Solution #20: E2E handling for interaction of AIoT Device related information

### 6.20.1 Description

The solution is to address KI#1#2#3.

The interaction for AIoT Device related information may happen between AIoT device and AIoT function or AF. Those AIoT Device related information includes:

- Device UL info which is from AIoT device and will be sent to AIoT function or AF.

- Device DL info which is from AIoT function or AF and will be sent to the AIoT device.

Generally, both Device UL info and Device DL info are transparent to the reader.

|  |
| --- |
| The legacy procedure for UE information interaction is as the following.   * Step1: After RRC establishment, the NG RAN node trigger initial UE message to the send the UE initial NAS information to the AMF * Step2: Based on the initial UE message, AMF setup UE association between the NG RAN node and the AMF. The subsequent UL and DL UE NAS PDU delivery use the UE association related signalling. |
| The UE association between RAN and AMF as described as the following: 9.3.3.1 AMF UE NGAP ID This IE uniquely identifies the UE association over the NG interface, as described in TS 38.401 [14].   |  |  |  |  |  | | --- | --- | --- | --- | --- | | IE/Group Name | Presence | Range | IE type and reference | Semantics description | | AMF UE NGAP ID | M |  | INTEGER (0..240 -1) |  |  9.3.3.2 RAN UE NGAP ID This IE uniquely identifies the UE association over the NG interface within the NG-RAN node.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | IE/Group Name | Presence | Range | IE type and reference | Semantics description | | RAN UE NGAP ID | M |  | INTEGER (0..232 -1) |  | |

W.R.T the Ambient IoT, there is also per AIoT device interaction although there is no RRC states for AIoT device, but the interaction for the AIoT device related information may happen in several rounds between AIoT device and AIoT Function or AF. E.g. authentication firstly and further read and/or write. Operation. But those detail can be transparent to the reader. So there also is requirement for per AIoT device association between the reader and the AIoT function to associate and ensure the interaction for AIoT Device related information.



Figure 6.20.1-1: interaction for AIoT Device related information

NOTE: The AS layer ID for AIoT Device is up to RAN WG decision. It is assumed the High layer ID (the layer above AS, e.g. NAS layer ID, or Application layer ID) for AS Device is transparent to the reader.

However, there might be thousands of AIoT devices that match the AIoT operation and it is not expected to setup thousands of per AIoT device association between the reader and AIoT function. And it delays much to setup the per AIoT device association after the reader receives the initial response from the AIoT device, since the association setup delay is probably longer than the delay to finish the interaction with an AIoT device.

Hence, it is proposed the following for the per AIoT device association between the reader and AIoT function:

- The AIoT function trigger to setup a list of per AIoT device association between the reader and AIoT function in advance.

- For each new discovered AIoT device (e.g. receiving the initial response from the AIoT device), the reader binds the AIoT device to a pre-setup per AIoT device association. The binding exists during the interaction with AIoT devices but doesn’t change the states of AIoT device, i.e. it is still no RRC state.

- After the interaction with the AIoT device finished, the binding is released and the per AIoT device association become available again and can be reused to bind another new discovered AIoT device.

- The pre-setup per AIoT device association doesn’t necessary to be the exact number for target AIoT devices that match the AIoT operation. E.g. pre-setup per AIoT device association is 50, but the potential AIoT devices of the AIoT operation may be 1000. Since the AIoT devices discovery procedure by the reader is one by one and number of AIoT devices under the reader’s operation in the meantime is limited, so the limited number of pre-setup per AIoT device association are sufficient and efficient to support the AIoT operation.

As shown figure 6.20.1-2, for one AIoT operation, the AIoT function can setup separate association with multiple readers for one AIoT operation session. And under each reader, a list of per AIoT Device association is pre-setup and will be used to associate and ensure the information related the discovered AIoT Devices. 

Figure 6.20.1-2: multiple per AIoT device Association within an AIoT operation

### 6.20.2 Procedures

#### 6.20.2.1 The interaction for AIoT Device among AIoT device, reader and AIoT Function



Figure 6.20.2.1-1: Service Flow

1. An AF requests AIoT operation to the AIoT Function directly or via NEF

2. AIoT Function allocates an AIoT operation session ID used for the once invoked AIoT operation request and it is used to associate the information related to AIoT operation during the AIoT operation session. The AIoT function requires the AIoT operation association setup to the selected readers, including: the AIoT operation session ID, AIoT operation information, a list of per AIoT device association setup requirement, etc.

3. The reader accepts to setup the AIoT operation association and a list of per AIoT device associations.

4. The reader uses the AIoT operation information to trigger AS AIoT signalling, including the AIoT operation session ID.

5. The AIoT Device-A feedback the initial response (Device-A UL Info, AS layer Device ID, AIoT operation session ID).

NOTE 1: Device-A presents one AIoT device. The AIoT operation session ID in step5 is the AIoT operation session ID received in step4. It is used by the reader to identify the related AIoT operation session and AIoT function that should receive the Device-A UL Info.

6. The reader binds new discovered Device-A to an available per AIoT device association.

NOTE 2: there might be multiple bind per AIoT device associations ongoing in the meantime.

7. The reader uses the bind per AIoT device association to forward the Device-A UL Info to the AIoT function which is determined via the AIoT operation session ID.

8. The AIoT function receives the Device-A UL Info from per AIoT device association and binds Device-A and the AIoT device association together.

9. If there is further info for Device-A, the AIoT function uses the bind per AIoT device association to forward the Device-A DL Info to the reader.

10. The reader forwards the received Device-A DL Info to Device-A based on the binding between Device-A and per AIoT device association.

11-12: The reader forwards the received Device-A UL Info to the AIoT funcion based on the binding between Device-A and per AIoT device association.

NOTE 3: Step9 to Step 12 may be repeated.

13-14. After finished the interaction with the AIoT device, the AIoT function can trigger to release the binding and the per AIoT device association becomes available again and can be used for another additional discovered AIoT device.

15. If the reader doesn’t receive new AIoT device response any more, the reader notifies the situation to the AIoT function. Based on the received notification, the AIoT function may update the AIoT operation information to the reader or end the AIoT operation with the reader. The AIoF Function may also notify the situation to the AF and let AF to determine update the AIoT operation information or end the AIoT operation.

16. When the AIoT operation ends, the AIoT function reports to AIoT operation result to the AF.

#### 6.20.2.2 The interaction for AIoT Device among AIoT device, reader, AIoT Function and AF.



Figure 6.20.2.2-1: Service Flow

1-8 are the same as Step1-8 as described in clause 6.20.2.2-1

9. If Device-A UL Info is for AF, the AIoT function forward it the AF with the AIoT operation session ID.

NOTE 1: Device-A present one AIoT device.10. Optionally, the AF may send to the AIoT function the Device-A DL Info with the AIoT operation session ID, or the AF notifies the AIoT function that the interaction with AIoT Device-A is finished.

11. The reader forwards the received Device-A DL Info to the reader based on the binding between Device-A and per AIoT device association.

12. The reader forwards the received Device-A DL Info to Device-A based on the binding between Device-A and per AIoT device association.

NOTE 2: The UL and DL interaction among AIoT Device, AIoT function and AF may be repeated.

13. After finished the interaction with the AIoT device, the AF notifies the AIoT function that the interaction with AIoT Device-A is finished.

14-15. The AIoT function can trigger to release the binding and the per AIoT device association becomes available again and can be used for another additional discovered AIoT device.

If the reader doesn’t receive new AIoT device response any more, the reader notifies the situation to the AIoT function. Based on the received notification, the AIoT function may update the AIoT operation information to the reader or end the AIoT operation with the reader. The AIoT Function may also notify the situation to the AF and let AF to determine update the AIoT operation information or end the AIoT operation.

### 6.20.3 Impacts on services, entities and interfaces

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

## 6.21 Solution #21: Architecture enhancement to support AIoT services for topology 2

### 6.21.1 Description

The solution applies to the Key Issue#1 "Architecture support of Ambient IoT Devices", 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 2 as defined in TR 38.848 [7].

The Figure 6.21.1-1 illustrates the system architecture to support AIoT services for Topology 2.



Figure 6.21.1-1: System Architecture to support AIoT Services for Topology 2

The system architecture and functions as defined in TS 23.501 [4] are used as basis to support the Ambient IoT services (e.g. Inventory, Command) with the following clarifications:

- AMF is enhanced to support transfer of service request from AF (via NEF) to UE, and transfer of service response from UE to AF (via NEF).

- NEF is enhanced to support transfer of service request from AF to AMF, and transfer of service response from AMF to AF.

- UDM is enhanced to support authorize AIoT service request from AF, and AIoT service response from UE.

- UE is enhanced to support Reader functions.

The Figure 6.21.1-2 illustrates the protocol stack to support AIoT services for Topology 2.



Figure 6.21.1-2: Protocol stack to support AIoT Services for Topology 2

As shown in the Figure 6.21.1-2, it is assumed AIoT Device communicates with UE via a new interface AIoT and both Access Stratum layer and Non-Access Stratum layer are supported. The UE communicates with the network using the existing Uu interface.

NOTE 1: The Access Stratum layer functionality is to be defined by RAN WGs.

For topology 2, the UE performs the Reader functions to send AIoT service request (e.g. Inventory, Command) to the AIoT Devices and receive AIoT service response (e.g. Device ID, AIoT data) from the AIoT Devices. The UE also acts as an intermediate node which is under the network control. This solution proposes a control plane based solution for core network to select the UE and to transfer the AIoT service request/response between UE and AF.

The AF requests service operation for an AIoT Device or a group of AIoT Devices or all of AIoT Devices via the NEF, and the NEF forwards the requested service operation to the AMF. The AMF selects the UE and delivers the requested service operation to the UE. The UE performs service operation (e.g. Inventory, Command) with the AIoT Devices and transfers the AIoT information (e.g. Device ID, AIoT data) received from the AIoT Devices to the AMF. The AMF then sends the AIoT information the AF via the NEF.

### 6.21.2 Procedures

Depicted in Figure 6.21.2-1 is the procedure to support AIoT Services for Topology 2.



Figure 6.21.2-1: Procedure to support AIoT Services for Topology 2

1. UE performs Registration procedure as defined in TS 23.502 [5]. The UE includes AIoT Communication Indication in the Registration Request message and the AIoT Communication Indication indicates whether UE supports communication with AIoT Devices. If the UE is authorized to communicate with the AIoT Devices, the AMF includes authorized information in the Registration Accept message to the UE.

2. AF sends an AIoT Service Request (AF Identifier, UE ID, Device ID, requested service operation, area information) message to the NEF. The requested service operation indicates the service (e.g. Inventory, Command) the AF requested for the Ambient IoT Device(s). Device ID is used to identify one/group/all of Ambient IoT Devices. The area information is used to indicate the area the service operation will be applied, and the area information could be geographic area. The UE ID is the GPSI of UE.

The service operation could be an end-to-end parameter between AF and Ambient IoT Device which means it is transparent to CN, NG-RAN and UE, it also could be a parameter that can be understood by CN and UE. The following steps further clarify how these two options work.

Editor's note: How does AF know whether UE is in the target area or not is FFS.

3. The NEF checks if the AF is authorized to request the AIoT service and requests for the serving AMF of the UE if UE ID is provided in step 2.

4. The NEF selects the AMF either using the serving AMF retrieved from UDM in step 3 or mapping the area information to the corresponding AMF, and forwards the requested service operation to the AMF using AIoT Service Request (Device ID, UE ID, requested service operation, RA list) message. The RA (Registration Area) list is mapped from area information and may also be included for UE selection by the AMF. The UE ID is SUPI of UE.

5. The AMF selects the UE (if not provided in step 4) for AIoT service operation if its registered area is in the RA list.

Editor's note: Other criteria and further details on UE selection is FFS.

6. The AMF may derive the service operation based on the requested service operation and include the service operation in a DL NAS message (Device ID, service operation) to the UE, or the AMF may include the requested service operation as a container in a DL NAS message (Device ID, service operation) to the UE. If the UE is in CM\_IDLE state, the network initiated service request procedure is performed before sending the DL NAS message.

7. The UE (Reader) performs AS procedure (e.g. paging-like procedure) with Ambient IoT Devices. The UE may include an AIoT-NAS message (Device ID, service operation) into the AS message to the Ambient IoT Devices.

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

9. The Ambient IoT Device sends and AIoT-NAS message (Device ID, AIoT data) over AS message. If the service operation is Inventory, the Device ID is included in the AIoT-NAS message. If the service operation is Command (e.g. Read), the AIoT data along with the Device ID are included in the AIoT-NAS message if requested by the service operation.

Editor's note: The security aspects of IoT-NAS message including group security is FFS.

NOTE 1: The AS procedures in steps 7, 8 and 9 are to be defined by RAN WGs.

NOTE 2: The security protection of AIoT-NAS message is to be designed by SA3.

10. The UE validates the Device ID which may require interaction with the core network.

Editor's note: The details on how does UE validate the Device ID and whether and how UDM is involved is FFS.

11. The UE sends an UL NAS message (Device ID, AIoT data) to the AMF.

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

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

### 6.21.3 Impacts on services, entities and interfaces

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

## 6.22 Solution #22: AF Based Solution for Topology 2

### 6.22.1 Description

#### 6.22.1.0 General

This solution proposes an AF based solution, which addresses KI#1, KI#2 and KI#3.

In this solution, it is AF who is in charge of the intermediate UE for the Ambient IoT operations, including communicating with and determining intermediate UEs, sending operation commands to and receiving results from intermediate UEs. As the licensed spectrum is owned by MNO, it is proposed to let network provide the radio resource information towards the intermediate UEs about the spectrum information for the over-the-air interface between Intermediate UEs and AIoT devices.

Editor's note: It is FFS about the improvements by locating more functions in CN, e.g., AF get locations of Intermediate UEs from CN but not from UEs; CN may determine Intermediate UEs on behalf of AF.

#### 6.22.1.1 Reference Architecture

The Figure 6.22.1.1-1 illustrates the architecture for AF based solution:



Figure 6.22.1.1-1: System Architecture of AF Based Solution

This solution focuses on Topology 2.

Editor's note: It is FFS whether and how the solution can be evolved for Topology 1.

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

- UDM/UDR: The authorization information of Intermediate UE for AIoT is stored in UE subscription data

- AMF: Receive AIoT capability information from UE and authorize based on the subscription data in UDM/UDR.

- NG-RAN: Provide spectrum information towards authorized intermediate UE.

- Intermediate UE:

- Provide Ambient IoT capability information to AMF and receive the authorization information

- Receive the instruction from AF and perform Ambient IoT operations (e.g., inventory, command, etc.) on the proper spectrum. The radio resource information is received from NG-RAN

- Receive command results from AIoT devices and send to AF.

- AF:

- UE AIOT layer interactions with Intermediate UEs

- Determine Intermediate UEs, send the instruction to the Intermediate UEs, and receive responses from Intermediate UEs.

Editor's note: Further involvement of the CN is FFS, including whether and how to perform access control for devices, and how to perform charging towards CHF.

#### 6.22.1.2 Protocol Stack

The Figure 6.22.1.2-1 illustrates the protocol stack for AF based solution over user plane:



Figure 6.22.1.2-1: Protocol Stack for AF Based Solution (over user plane)

Within the protocol stack:

- UE AIoT layer: between AF and UE reader. AF provides Ambient IoT operation commands to Intermeidate UEs via UE AIoT layer.

- Command layer: The command layer protocol between AIoT devices and AF, including, e.g., read, write, execute, etc.

- Uu AS layer: On top of the existing Uu AS layer, radio resource information request from UE reader to NG-RAN.

It is assumed that the end-to-end protection is implemented between AF and AIoT devices.

NOTE 1: The UE AIOT layer and Command layer are assumed to be defined by SA2 (Stage 2 aspects) and CT1 (Stage 3 aspects) but can be determined during conclusion phase.

NOTE 2: The Details of the protection between AIoT device and AF and the protection between AIoT device and UE reader are assumed to be addressed by SA3.

The UE AIOT layer messages between AF and UE reader can be transferred via PDU session user plane. AF delivers downlink messages towards Intermediate UE and receives uplink messages from Intermediate UE via UPF.

The protocol stack for AF Based Solution over control plane is similar, with the involvement of CN control plane NFs (AMF, SMF, NEF) instead of user plane NF (UPF). Over control plane, UE AIOT layer is over the NAS layer in UE reader. AF communicates with UE reader via control plane, by utilizing the Control Plane CIoT 5GS Optimisation. The downlink messages are sent by AF, and delivered through NEF, SMF, AMF, NG-RAN towards Intermediate UE. The uplink messages are sent by the Intermediate UE, and delivered through NG-RAN, AMF, SMF, NEF towards AF.

### 6.22.2 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.

#### 6.22.2.1 AIoT Service Authorization for Intermediate UE

The Registration procedure for UE is performed as defined in clause 4.2.2.2 of TS 23.502 with the following additions:

- UE includes the AIoT Intermediate node capability as part of “5GMM capability” in Registration Request message.

- The AMF obtains the AIoT Subscription data as part of the user subscription data from UDM using Nudm\_SDM service

- The AMF determines whether the UE is authorized to work as Intermediate UE for AIoT based on UE’s AIoT Intermediate node capability and the AIoT Subscription data. The AMF includes the authorization information as part of UE context in NGAP message sent to NG-RAN.

In Service Request procedure, N2 Handover prodcure, Xn Handover procedure, and when receiving Subscriber Data Update to AMF, the AMF includes the authorization information in NGAP message sent to NG-RAN.

#### 6.22.2.2 Inventory Procedure

The Inventory procedure can be initiated by the AF to discover one or more AIoT devices in a specific area via Intermediate UEs.



Figure 6.22.2.2-1: Inventory Procedure

1. Via the Intermediate UE’s PDU session user plane or control plane, the Intermediate UE communicates with the AF to transport UE AIOT layer messages, including location information reporting and reader capability information.

2. The AF determines Intermediate UEs based on the location information and reader capability information reported by the Intermediate UEs in step 1, as well as the area AF intended to perform inventory.

Editor's note: It is FFS on whether and how the posture information of Intermediate UEs can be collected and the impacts on the determination of Intermediate UEs.

3. The AF sends Inventory Request towards the selected Intermediate UEs via Core Network and NG-RAN over PDU session user plane or control plane. The Inventory Request includes the device information, inventory strategy information.

- The device information could be device ID, device group ID, and/or device type. The device type refers to type 1, 2A or 2B in TR 38.769 [8].

NOTE 1: It’s up to RAN to determine whether the device type is useful or not for Intermediate UE, based on the assumption of harmonized air interface.

- The inventory strategy information contains, e.g., the inventory frequency and inventory period to guide the reader 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. For flexibility, the delta inventory may require the device to respond if it is reading by a different reader, even if the device has performed the inventory procedure, which requires the AIoT devices to keep the reader ID.

- 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.

4. The Intermediate UE interacts with NG-RAN for radio resource allocation

NOTE 2: The detail of this function is assumed to be defined by RAN.

5. The Intermediate UE initiates inventory based on device information as well as the inventory strategy information provided by the AF. To be able to differentiate readers in delta inventory, the Intermediate UE may provide reader identity information to enable the AIoT devices to understand they are read by which Intermediate UE. Considering the mobility of the Intermediate UE (e.g., when the Intermediate UE and some devices move together to another room, in the following delta inventory, the devices can regard the Intermeidate UE in a new room as a different reader than the one they have responded), the reader identity information can be a combination of an application layer reader ID and the location information.

6. The AIoT Device reports the device ID. 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 reader, it should skip the reporting.

7. The Intermediate UE may perform aggregation for the device ID, based on the report aggregation information provided by the AF. Within the aggregation period, the Intermediate UE will buffer the device IDs reported from the AIoT devices. The Intermediate UE may stop buffering and send report immediately, if it determines no further report from devices. When the aggregation period expires, the Intermediate UE sends the report. For those device ID report after the aggregation period, if it is needed by the AF, the Intermediate UE sends the report. Otherwise, it will be dropped.

8. The Intermediate UE sends Inventory Response or Notification Request towards the AF for the device ID or the aggregated device ID information.

The Intermediate UE may perform periodic inventory following the instructions from AF, as described in Solution#8.

#### 6.22.2.3 Command Procedure

The Command procedure is initiated by the AF to request one or more AIoT devices in a specific area to execute a command via Intermediate UEs. The device may or may not send back the command results depends on the command.



Figure 6.22.2.3-1: Command Procedure

1. Via the Intermediate UE’s PDU session user plane or control plane, the Intermediate UE communicates with the AF to transport UE AIOT layer messages, including location information reporting and reader capability information.

2. The AF determines Intermediate UEs based on the location information and reader capability information reported by the Intermediate UEs in step 1, as well as the area AF intended to perform command.

3. The AF sends Command Request towards the selected Intermediate UEs via Core Network and NG-RAN over user plane or control plane. The Command Request includes the command, device information, result aggregation information.

- The command is the command to be executed in the device, including read, write, enable, disable, or other application specific command.

- The device information could be device ID, device group ID, and/or device type. The device type refers to type 1, 2A or 2B in TR 38.769 [8].

NOTE 1: It’s up to RAN to determine whether the device type is useful or not for Intermediate UE, based on the assumption of harmonized air interface.

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

4. The Intermediate UE interacts with NG-RAN for radio resource allocation

NOTE 2: The detail of this function is assumed to be defined by RAN.

5. The Intermediate UE delivers the command to the AIoT devices.

6. The AIoT Device executes the command and send back the result to the Intermediate UE if needed.

7. The Intermediate UE may perform aggregation for the result, based on the report aggregation information provided by the AF. Within the aggregation period, the Intermediate UE will buffer the results from the AIoT devices. The Intermediate UE may stop buffering and send report immediately, if it determines no further results from devices. When the aggregation period expires, the Intermediate UE sends the report. For those results after the aggregation period, if it is needed by the AF, the Intermediate UE sends the report. Otherwise, they will be dropped.

8. The Intermediate UE sends Command Response or Notification Request towards the AF for the result or the aggregated results.

### 6.22.3 Impacts on services, entities and interfaces

The following NFs are impacted:

- UDM/UDR: Store the authorization information of Intermediate UE for AIoT

- AMF: Receive AIoT capability information from UE and authorize based on the subscription data in UDM/UDR.

- NG-RAN: Provide spectrum information towards authorized intermediate UE.

- Intermediate UE:

- Provide Ambient IoT capability information to AMF and receive the authorization information

- Receive the instruction from AF and perform Ambient IoT operations (e.g., inventory, command, etc.) on the proper spectrum. The radio resource information is received from NG-RAN

- Receive responses from AIoT devices and send to AF.

- AF:

- UE AIOT layer interactions with Intermediate UEs

- Determine Intermediate UEs, send the instruction to the Intermediate UEs, and receive responses from Intermediate UEs.

## 6.23 Solution #23: UE reader selection for inventory procedure

### 6.23.1 Description

#### 6.23.1.1 Definition

**AIoT device capability**: e.g. inventory frequency, etc. Different AIoT devices may support different inventory frequency.

**reader**: part of the intermediate node UE, which can communicate with the AIoT device via radio interface;

**UE reader capability**: e.g. inventory frequency, etc. Different readers may support different inventory frequencies, and the inventory frequency supported by the reader may be different from the inventory frequency supported by the AIoT device as well. To execute the inventory related procedure between the device and the reader, the inventory frequency used by the device and the reader should match with each other;

#### 6.23.1.2 General

This solution applies to Key issue #3 in terms of selecting the reader used for Ambient IoT inventory service.

This solution applies to the following scenario:

- The AF (i.e. third party) uses a bulk of AIoT devices that have the same AIoT device capabilities, e.g. the same inventory frequency, etc;

- the AF holds the AIoT device information (e.g. device capabilities, etc.).

This solution applies to topology 2.

This solution proposes to select the appropriate UE readers before performing the inventory procedure.

#### 6.23.1.3 Architecture and Principles



Figure 6.23.1.3-1: Reference architecture

The principles of the solution:

- AF provides the AIoT device capability to the Ambient IoT Function (AIoTF);

- the selection of the intermediate node UE will be based on: the AIoT device capability, the inventory area wherein the AIoT devices are supposed to be, and the the UE reader capability;

- AIoTF is responsible for:

- mapping the third party information (e.g. the inventory area information) to 3GPP information (e.g. cell ID, etc);

- selecting the appropriate intermediate node UE;

### 6.23.2 Procedures

This clause provides how to select the UE readers that will be used for the inventory procedure.



Figure 6.23.2-1: UE reader selection procedure

1. The intermediate node UE performs the registration procedure. The AIoT UE reader capabilities (e.g. supported inventory frequency) will be transmitted to the AMF via the NAS message (e.g. the Registration Request message).

2. The AF sends to the AIoTF the inventory request information that includes: inventory area information, AIoT device capabilities (e.g. supported frequency, etc.), etc. The inventory area information defined by the third party indicates the area where the AIoT devices are supposed to be.

Editor's note: It is FFS how the AF selects AIoTF if multiple AIoTFs are deployed in the core network.

3. The AIoTF maps the third party defined information into the information defined in 3GPP. For example, the inventory area information is mapped into the cell ID which could help the AIoTF to select the AMF.

Editor's note: It is FFS how the AIoTF selects AMF if multiple AMFs serve the same area.

4. The AIoTF get from the AMF the information of the intermediate node UEs that are available in the cell with the cell ID mapped in step 3. The information of the intermediate node UE includes: e.g. UE ID, inventory frequency;

5. The AIoTF selects the appropriate intermediate node UEs that will be engaged in the inventory procedure. The inventory frequency of the intermediate UE should overlap with the inventory frequency supported by the AIoT device.

6. The inventory procedure is carried out. The radio configuration (inventory frequency, etc.) of the intermediate node, e.g. how RAN to schedule the radio resource to reader UE, is up to RAN WGs.

NOTE: It depends on operator's policy or configuration that there can be different selection criteria of the intermediate node, e.g. based on the frequency capability of the AIoT device and the intermediate node.

Editor's note: It is FFS how the inventory procedure is carried out in terms of other aspects.

### 6.23.3 Impacts on services, entities and interfaces

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

## 6.24 Solution #24: Availability Reporting without Ambient IoT Device Timers

### 6.24.1 Functional Description

This solution focuses on the registration management and/or connection management aspects of Key Issue #2 "Identification, Subscription, Registration and Connection management".

The main principle of the proposal is that the architecture should support a way for the Ambient IoT Device to determine when it needs to perform a control plane procedure without requiring the Ambient IoT device to always run timers (e.g. a periodic registration timer).

In this solution, the network can send a “check-in” time value to the Ambient IoT Device in any procedure. The Ambient IoT Device stores the time value while it sleeps and does not have to run any timers. When the Ambient IoT Device wakes up from a sleep state, the Ambient IoT Device will read time information that is broadcasted from the network or an intermediate node. If the broadcasted information indicates that the time is past the “check-in” time, then the Ambient IoT Device will initiate a control plane procedure.

This approach will help ensure that the Ambient IoT Device will not go a long period of time without announcing its availability (e.g. registering) and will also help ensure that the Ambient IoT Device does not initiate control plane procedures too often.

### 6.24.2 Procedures

Figure 6.24.2-1 shows the procedure.



Figure 6.24.2-1: Procedure for Ambient IoT Device Availability Reporting

1. Upon network or IN trigger (e.g., activation signal, inventory request, not shown in the figure) the Ambient IoT Device sends a control plane request to the network. For example, it may be a device Registration request or a Inventory report. This control plane request informs the network that the Ambient IoT Device is still present in the network..

2. The Ambient IoT Device receives a control plane response from the network. The response includes an absolute time value. The time value indicates to the Ambient IoT Device that the device should send another control plane request sometime after the time value. The network node that assigns the time value depends on the overall architecture of the network that the Ambient IoT Devices connect to, but would most likely be the network function where control plane messages terminate and/or the network function that keeps track of Ambient IoT Device’s presence in the network.

The Ambient IoT Device is allowed to initiate a control plane request before the time value, for example, to report a detected event. However, the time value will help ensure that the Ambient IoT Device will not go a long period of time without announcing its availability (i.e. registering) and will also help ensure that the Ambient IoT Device does not initiate control plane procedures too often.

3. The Ambient IoT Device enters the sleep state. Timers do not need to run in the Ambient IoT Device and no real-time clock needs to be maintained by the Ambient IoT Device.

4. The Ambient IoT Device is energized or triggered. The trigger could be an activation signal that is received from the Network or Intermediate Node.

5. The Ambient IoT Device wakes up because of the trigger.

6. The Ambient IoT Device reads time information that is broadcasted by the Network or Intermediate Node. If the time information indicates that the current time is earlier than the time value that was received in Step 2, then the Ambient IoT Device can return to the sleep state of Step 3. If the time information indicates that the current time is equal to or later than the time value that was received in Step 2, then the Ambient IoT Device indicates its availability to the network by proceeding to Step 7.

7. In response to 4a/4b trigger, the Ambient IoT Device sends a control plane request to the network.

8. The network updates the device’s availability info (e.g., its current area, associated Reader, etc.). The network may take the opportunity to send data in a response or new request to the device. The response or new request may include a new time value.

NOTE: If the network doesn’t receive the device’s check-in message long after the check-in time, the network may consider the device not present in the network.

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

Network:

* Sends a time value to the Ambient IoT Device.

RAN/Intermediate Node UE:

* Broadcast time information

Ambient IoT Device:

* Receives and stores a time value from the network.
* Reads broadcasted time information.
* Compares the broadcasted time information with the value that was received from the network and uses the comparison to detect if it needs to send a control plane request.

## 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 A: Overview of the Electronic Product Code

The EPC Tag Data Standard [10], issued and maintained by the GS1 organisation [11], defines the Electronic Product Code as follows:

*The EPC is a universal identifier that provides a unique identity for any physical object. The EPC is designed to be unique across all physical objects in the world, over all time, and across all categories of physical objects. It is expressly intended for use by business applications that need to track all categories of physical objects, whatever they may be.*

In line with this definition, it is important to emphasize that the EPC Tag Data Standard [10] defines EPC as a means for unique identification of physical objects independently of any technology for storing and transmitting such EPC information. In other words, EPCs can be used independently of existing RFID tags.

Despite the word "product" that is an integral part of the term Electronic Product Code, EPCs are not only used for instance for retail items. Instead, the EPC Tag Data Standard [10] defined identification schemes for various business domains to enable identification of

- individual trade items based on the Serialised Global Trade Item Number (SGTIN) EPC scheme;

- logistics handling units (e.g., a pallet load) based on the Serial Shipping Container Code (SSCC) EPC scheme;

- returnable assets such as boxes, pallets and casks based on the Global Returnable Asset Identifier (GRAI);

- aircraft parts based on the Aerospace and Defense Identifier (ADI) EPC scheme;

- patients and the services provided to them based on the Global Service Relation Number (GSRN) EPC scheme (see also [12] for more information on the use of EPC in the healthcare supply chain);

- etc.

The reason that EPCs are unique despite being used by independently operating organizations in many different domains is the typical structure of the underlying EPC schemes, which typically include an organizational identifier.

For example, as illustrated in Fig. A-1, the Serial Shipping Container Code (SSCC) as defined in clause 6.3.2 of the EPC Tag Data Standard [10], consists of a GS1 Company Prefix and a Serial Reference. The GS1 Company Prefix number space is managed by the GS1 organization, which assigns GS1 Company Prefix numbers to individual organizations. The serial reference is then assigned by the organization itself. Together this yields a unique EPC.

|  |  |
| --- | --- |
| GS1 Company Prefix | Serial Reference |

Fig A-1: Serial Shipping Container Code EPC scheme.

The EPC Tag Data Standard [10] follows the same approach also for other EPC schemes, e.g., the Serialised Global Trade Item Number (SGTIN), which is used for individual trade items such as an instance of a specific product (e.g., an individual TV). As depicted in Fig. A-2, the SGTIN also contains a unique GS1 Company Prefix. In addition, the SGTN contains the Item Reference (to differentiate different object classes) and a Serial number, which are assigned by the organization identified by the company prefix.

|  |  |  |
| --- | --- | --- |
| GS1 Company Prefix | Item Reference | Serial Number |

Fig A-2: Serialised Global Trade Item Number (SGTIN) EPC scheme.

In clause 14, the EPC Tag Data Standard [10] also defines a binary encoding of the EPC schemes, i.e., the standard also defines how EPCs are serialized as a string of bits, e.g., for storage on tags.

As shown in Fig. A-3, the key idea is that a binary representation of an EPC starts with a header value that indicates the EPC scheme followed by the bitwise representation of a particular encoding scheme. For instance, SSCC-96 defines how the GS1 Company Prefix and the Serial Reference of the Serial Shipping Container Code are represented as a string of bits. The typical size of EPCs, e.g., for the Serialised Global Trade Item Number using the SGTIN-96 coding scheme is 96 bits (including the Header value).

|  |  |  |
| --- | --- | --- |
| EPC scheme | Header value | Coding scheme specific bits |
| Serial Shipping Container Code (SSCC) | 0011 0001 | SSCC-96 as defined in clause 14.6.2.1 of [10] |
| Serialised Global Trade Item Number (SGTIN) | 0011 0000 | SGTIN-96 as defined in clause 14.6.1.1 of [10] |

Fig A-3: The EPC binary representation consists of the header value that identifies the EPC scheme and coding scheme specific bits, e.g. SSCC-96 for the Serial Shipping Container Code as defined in [10]. (Note: This table shows a subset only.)

Annex B:  
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, S2-2403719, S2-2403429, S2-2403430, S2-2403431, S2-2403469, S2-2403471, S2-2403472, S2-2403473, S2-2403474, S2-2403475, S2-2403720, S2-2403721, S2-2403722. | 0.2.0 |
| 2024-04 | SA2#162 |  |  |  |  | Inclusion of documents approved in SA2#162:  S2-2405129, S2-2405130, S2-2405468, S2-2405470, S2-2405471, S2-2405472, S2-2405473, S2-2405474, S2-2405475, S2-2405476, S2-2405477, S2-2405478, S2-2405479, S2-2405480, S2-2405732, S2-2405733 | 0.3.0 |