|  |  |
| --- | --- |
| 3GPP TR 23.700-30 V0.2.0 (2025-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Architecture support of Ambient power-enabled Internet of Things (AIoT);  Phase 2;  (Release 20) | |
|  | |
|  |  |
|  |  |
|  | |
| 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.  © 2025, 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, symbols 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 10

5 Key Issues 11

5.1 Key Issue #1: support AIoT services under the RRC-based option for UE Reader connectivity 11

5.2 Key Issue #2: Support of DO-A Capable AIoT Devices 11

6 Solutions 12

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: Enable 5G delivery AIoT device initiated traffic 12

6.1.0 High-level solution principles 12

6.1.1 Description 13

6.1.2 Procedures 14

6.1.3 Impacts on Services, Entities and Interfaces 16

6.2 Solution #2: AIoT services support for DO-A capable AIoT Devices 16

6.2.0 High-level Solution Principles 16

6.2.1 Description 17

6.2.2 Procedures 17

6.2.3 Impacts on Services, Entities and Interfaces 18

6.3 Solution #3: Support of Sensor Data Collection 18

6.3.0 High-level solution Principles 18

6.3.1 Description 18

6.3.2 Procedures 19

6.3.3 Impacts on services, entities and interfaces 20

6.4 Solution #4: Architecture enhancements to support DO-A capable devices 21

6.4.0 High-level solution Principles 21

6.4.1 Description 21

6.4.2 Procedures 22

6.4.2.1 Ambient IoT device registration and DO-A execution 22

6.4.2.2 AIoT device capability syncronization 23

6.4.3 Impacts on Services, Entities and Interfaces 24

6.5 Solution #5: DO-A procedure with configured routing information 24

6.5.0 High-level solution Principles 24

6.5.1 Description 24

6.5.2 Procedures 25

6.5.2.1 DO-A data subscribe procedure 25

6.5.2.2 DO-A data transfer procedure 26

6.5.3 Impacts on services, entities and interfaces 27

6.6 Solution #6: Support Reporting operator triggered by events without registration for DO-A capable AIoT Devices 28

6.6.0 High-level Solution Principles 28

6.6.1 Description 28

6.6.2 Procedures 28

6.6.3 Impacts on Services, Entities and Interfaces 29

6.7 Solution #7: DO-A procedure for DO-A Capable AIoT Devices 30

6.7.0 High-level solution Principles 30

6.7.1 Description 30

6.7.2 Procedures 31

6.7.3 Impacts on services, entities and interfaces 32

6.8 Solution #8: Service Procedure for DO-A Capable AIoT Devices 33

6.8.0 High-level solution Principles 33

6.8.1 Description 33

6.8.2 Procedures 34

6.8.2.1 Initiating message and data transfer procedure 34

6.8.2.2 AF subscription procedure 36

6.8.3 Impacts on Services, Entities and Interfaces 36

6.9 Solution #9: Autonomous registration and data transfer from AIoT Device 37

6.9.0 High-level solution Principles 37

6.9.1 Description 37

6.9.2 Procedures 37

6.9.2.1 DO-A procedure for Topology 1 38

6.9.2.2 DO-A procedure for Topology 2 39

6.9.3 Impacts on services, entities and interfaces 41

6.10 Solution #10: DO-A Data Delivery and Routing 41

6.10.0 High-level Solution Principles 41

6.10.1 Description 41

6.10.2 Procedures 42

6.10.2.1 Subscribe to DO-A Data Delivery 42

6.10.2.2 DO-A Data Delivery 43

6.10.3 Impacts on Services, Entities and Interfaces 44

6.11 Solution #11: DO-A device registration and uplink data transmission 44

6.11.0 High-level Solution Principles 44

6.11.1 Description 45

6.11.2 Procedures 46

6.11.3 Impacts on Services, Entities and Interfaces 47

6.12 Solution #12: Enable DO-A traffic with MICO like mechanism 48

6.12.1.1 High-level solution principles 48

6.12.1.2 Definition 48

6.12.2.1 enhanced command procedure to configure AIoT device 49

6.12.2.2 DO-A procedure 50

6.13 Solution #13: Network Triggered Initial Registration 52

6.13.0 High-level solution principles 52

6.13.1 Description 53

6.13.2 Procedure 54

6.13.3 Impacts on Services, Entities and Interfaces 55

6.14 Solution #14: DO-A capable AIoT Device Registration Procedure 56

6.14.0 High-level solution Principles 56

6.14.1 Description 56

6.14.2 Procedures 57

6.14.3 Impacts on Services, Entities and Interfaces 58

6.15 Solution #15: Support reliable time-base Data Collection of DO-A AIoT sensor device with network trigger 59

6.15.0 High-level solution Principles 59

6.15.1 Description 59

6.15.2 Procedures 59

6.15.3 Impacts on services, entities and interfaces 61

6.16 Solution #16: AIoT device DOA data detection and collection 61

6.16.0 High-level solution Principles 61

6.16.1 Description 62

6.16.1.1 Device broadcasted “Data Ready Indication” 62

6.16.1.2 Enhanced R19 AIoT Paging and Command procedures for collecting DOA data 62

6.16.1.3 Routing of DOA data 62

6.16.2 Procedures 63

6.16.3 Impacts on Services, Entities and Interfaces 64

6.17 Solution #17: Service aspects for DO-A traffic in Ambient IoT networks 65

6.17.1 High-level solution principles 65

6.17.1 Description 65

6.17.2 Procedures 65

6.17.2.1 Configuring the network to support DO-A support as a service 65

6.17.3 Impacts on Services, Entities and Interfaces 66

6.18 Solution #18: AIoT Device Registration and data transmission Procedure 67

6.18.0 High-level solution Principles 67

6.18.1 Description 67

6.18.2 Procedures 68

6.18.2.1 Registration Procedure 68

6.18.2.3 DO-A traffic routing 70

6.18.2.4 Inventory Procedures 70

6.18.2.5 Command Procedures 70

6.18.3 Impacts on Services, Entities and Interfaces 71

6.X Solution #X: <Solution Title> 71

6.X.0 High-level solution Principles 71

6.X.1 Description 71

6.X.2 Procedures 71

6.X.3 Impacts on Services, Entities and Interfaces 72

7 Interim agreements 72

7.1 Agreed Principles 72

7.1.1 Agreed Principles for KI#1 72

7.2 Topics for further consideration 74

7.2.Z Topics for further consideration for KI#Z 74

8 Conclusions 74

Annex A: Change History 75

# 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 additional architecture support of Ambient IoT for the support of Rel-19 AIoT Devices defined in TS 23.369 [3] in Topology 2 based on the RRC-based option as described in clause 8.1.3.3 of TR 23.700‑13 [7] and support for new AIoT Devices that will support the DO-A traffic type as described in the "RAN WID Solutions for Ambient IoT (Internet of Things) in NR Phase 2" RP-251885 [9] and "RAN SID Study on enhancements for solutions for Ambient IoT (Internet of Things) in NR outdoor for active devices" RP-251884 [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 TS 23.369: "Architecture support for Ambient power-enabled Internet of Things; Stage 2".

[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 23.700‑13: "Study on Architecture support of Ambient power-enabled Internet of Things".

[8] 3GPP RP-251884: "New SID on enhancements for solutions for Ambient IoT (Internet of Things) in NR outdoor for active devices".

[9] 3GPP RP-251885: "New WID on Solutions for Ambient IoT (Internet of Things) in NR Phase 2".

[10] 3GPP TR 38.848: "Technical Specification Group Radio Access Network; Study on Ambient IoT (Internet of Things) in RAN".

[11] 3GPP TS 33.369: "Security aspects of ambient IoT services in 5G".

# 3 Definitions of terms, symbols 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].

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 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].

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Architectural Assumptions and Requirements

## 4.1 Architectural Assumptions

The following traffic types for AIoT Device are to be studied:

- DT: Device-terminated;

- DO-DTT: Device-originated - device-terminated triggered; and

- DO-A: Device-originated - autonomous.

Common architectural assumptions:

- Architecture reference models defined in TS 23.369 [3] are used as the baseline architecture for this study.

- The AIoT Device is agnostic to topologies, i.e. Topology 1 and Topology 2.

Architectural assumptions for support of Topology 2 for Key Issue#1:

- No Rel-19 AIoT Device impact is expected.

- The following topology as defined in TR 38.848 [10] is assumed:

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

- Only Indirect Connectivity (i.e. NG-RAN <-> AMF <-> AIOTF) is applied.

- The support of Topology 2 in this study is based on the RRC-based option and the interim conclusions of Rel-19 in TR 23.700-13 [7] is the baseline.

Architectural assumptions for support of DO-A Capable AIoT Devices:

- The AIoT Device is agnostic to Topology 1 architecture types, i.e. Direct Connectivity architecture and Indirect Connectivity architecture.

NOTE 1: Coordination with RAN WGs is required to determine the AIoT Device capabilities in relation to system level of functionality (considering e.g. traffic scenarios, connectivity topologies, etc.).

NOTE 2: The security aspects for Ambient IoT require coordination with SA WG3.

NOTE 3: The charging aspects for Ambient IoT will be studied by SA WG5.

## 4.2 Architectural Requirements

The following architectural requirements are applicable to this study:

- Solutions shall build on the 5G System architectural principles as in TS 23.501 [4], including flexibility and modularity for newly introduced functionalities.

- The enhancements to support topology 2 shall not impact Rel-19 AIoT devices.

- Solutions shall build on the AIoT architectural principles as in TS 23.369 [3].

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

NOTE: Privacy protection and other security aspects will be coordinated with SA WG3.

# 5 Key Issues

## 5.1 Key Issue #1: support AIoT services under the RRC-based option for UE Reader connectivity

NOTE 1: Only CM-CONNECTED with RRC\_CONNECTED UE Reader is in the scope.

Only the following aspects will be included:

- How to perform and revoke authorization of UE Readers.

NOTE 2: Rel-19 interim conclusion in TR 23.700-13 [7] should be used as basis for UE Reader authorization.

- Potential impact from how the NG-RAN node and UE reader selection can be performed.

NOTE 3: The aspect of NG-RAN node and UE reader selection requires coordination with RAN WG3.

- Whether and how the AIOTF can provide the information of the UE readers to the NG-RAN node to assist NG-RAN for UE reader selection.

NOTE 4: Rel-19 interim conclusion in TR 23.700-13 [7] should be used as basis for this key issue. No Rel-19 AIoT Device impact from this key issue is expected.

NOTE 5: Conclusions of this KI will be coordinated with RAN WGs.

## 5.2 Key Issue #2: Support of DO-A Capable AIoT Devices

This key issue will study the system architecture to support DO-A capable Ambient IoT Devices in Topology 1 and Topology 2.

The following aspects will be studied:

- How the AIoT Device informs the network of its presence autonomously (e.g., an AIoT Device initiated registration-like procedure) and what are the triggers for the DO-A capable device to inform the network of its presence.

- Whether and how to consider power consumption of DO-A Capable AIoT Devices.

- How an AIoT Device sends data to the AIOTF autonomously.

- Support for routing the data received by AIOTF from an AIoT Device to an AF.

- Whether and how to enhance the Inventory and Command procedures defined in TS 23.369 [3] to support DO-A capable AIoT Devices.

- Naiotf, Namf and Nnef interface enhancements to support DO-A capable AIoT Device.

NOTE 1: The conclusions from Key Issue #1 are the basis for supporting DO-A capable AIoT Devices in topology 2 in this key issue.

NOTE 2: Coordination with RAN WGs is required.

# 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 |
| #1 |  | X |
| #2 |  | X |
| #3 |  | X |
| #4 |  | X |
| #5 |  | X |
| #6 |  | X |
| #7 |  | X |
| #8 |  | X |
| #9 |  | X |
| #10 |  | X |
| #11 |  | X |
| #12 |  | X |
| #13 |  | X |
| #14 |  | X |
| #15 |  | X |
| #16 |  | X |
| #17 |  | X |
| #18 |  | X |

## 6.1 Solution #1: Enable 5G delivery AIoT device initiated traffic

### 6.1.0 High-level solution principles

The key technical principles proposed in this solution are summarized below:

1. AIoT Device Profile Enhancement: The AIoT Device Profile is extended to include additional information, such as AF/NEF associations and the device’s registration status.

2. Device Registration Requirement: Each AIoT Device must be registered with the 5G network to enable support for DO-A traffic.

3. Energy-Aware Communication Initiation: An AIoT Device may initiate communication when sufficient energy is available from non-RF sources. The device can also request the network to supply energy for subsequent transmissions by indicating its Active Time.

4. Redundant Traffic Management: The NG-RAN can identify and suppress redundant transmissions originating from multiple readers, indicating which reader is selected for subsequent forwarding. Readers maintain a local device context to prevent unnecessary traffic duplication.

5. Per-Device Session Context at AIOTF: The AIOTF maintains a session context for each device, including session IDs that allow subsequent messages to bypass repeated authorization and NEF discovery, improving efficiency.

6. Timestamp-Based Deduplication and Data Integrity: Each message carries a timestamp to enable detection and elimination of duplicate data, supporting network-side data cleaning and ensuring consistency.

NOTE: The feasibility of using timestamp depends on the RAN WGs.

7. NEF Selection Based on Device Profile: The AIOTF determines the appropriate NEF for forwarding traffic based on the AIoT device profile and the requested AF.

### 6.1.1 Description

The introduction of Device Oriented-Autonomous (DO-A) traffic type addresses a significant gap in AIoT networks, where devices initiate communication autonomously based on available energy resources. This capability was not supported in previous releases and is now within the scope of this Release. The proposed solution outlines a series of procedures that enable efficient handling of DO-A traffic, ensuring optimized network resource utilization.

Key Procedures:

1. AIoT Device Profile enhancement: the AIoT device profile stored in the ADM is enhanced to also include supported AF IDs along with their corresponding NEF IDs, and the AIoT device registration status.

2. Registration and Context Creation: AIoT devices register with the network by sending their device ID, which is encapsulated and forwarded through network elements for security validation. Upon successful authentication, the device profile is updated, and a context is created, detailing registration status and access permissions.

3. DO-A Traffic Initiation: When an AIoT device has sufficient energy, it autonomously initiates communication by sending a DO-A request message. This message includes device identification, a timestamp for data management, and an Active Time parameter indicating communication duration capability.

4. Traffic Routing and Optimization: The network elements, including AIoT readers and NG-RAN, manage traffic routing, ensuring efficient handling of DO-A messages. Duplicate data is identified and managed using timestamps, and session IDs are allocated for ongoing communications.

5. Authorization and Forwarding: The AIOTF verifies device context and authorizes traffic based on stored profile data. It forwards authorized traffic to the appropriate NEF, which then communicates with the requested AF.

6. Session Management: Subsequent communications utilize allocated session IDs, streamlining authorization processes and enabling direct traffic forwarding to known NEFs.

This proposal aims to enhance AIoT network functionality by supporting autonomous device communication, optimizing energy use, and improving network efficiency.

### 6.1.2 Procedures



Figure 6.1.2-1: Procedure for Enable 5G delivery AIoT device initiated traffic

0. The AIoT device profile per an AIoT device is provisioned in the ADM (AIoT specific UDM). The AIoT device profile includes the following parameters:

- AIoT Device Permanent ID: Uniquely identifies the AIoT Device.

- Last known AIOTF information: Indicates the last known AIOTF that served the AIoT device, or unknown.

- AF ID together with NEF ID: Indicates which AFs the AIoT device is allowed to access and which NEFs are used for communication with the AFs.

- Registration status: Indicates if the AIoT device is already registered with the network or not.

1. The AIoT device performs registration by sending a message containing its AIoT device ID to the AIoT reader. The reader forwards this message to the NG-RAN, which then passes it to the AIOTF for security validation. Upon successful authentication, the AIOTF updates the device profile status with the ADM, which responds with the updated profile data, including AF and NEF IDs, and provides a registration response message, which includes the registration result indicating whether it was successful or not to the AIoT device via the NG-RAN as well as the AIoT reader.

2. The AIOTF generates the AIoT device context which includes whether it is registered, which AFs it can access, and which NEFs should be used to communicate with the AFs.

3. When the AIoT device has something to send the network and has enough energy to do so, it initiates communication by sending the DO-A (Device Oriented-Autonomous) request message. This message includes the AIoT device ID (e.g., temporary ID, if it has been allocated by the network during the registration already) for the network to identify the AIoT device, timestamp indicating when this message was initiated, and the AIoT NAS message for the actual communication with the network and the AF (data consumer). The timestamp is later used by the network to perform data cleaning (e.g., removing data duplications). And the AIoT device ID and timestamp are not part of the AIoT NAS message to ensure they are understood by the AIoT reader and NG-RAN for proper traffic routing and optimization. The AIoT device also includes an Active Time parameter, which indicates how long the device can remain active to communicate with the network for subsequent messages. This Active Time can be zero if the AIoT device only had enough energy to send a single DO-A message.

4. The AIoT reader forwards the AIoT NAS message encapsulated over RRC to the serving NG-RAN. Additionally, the AIoT reader may send its AIoT reader ID, and the received AIoT device ID and timestamp.

5. The NG-RAN optionally checks if multiple AIoT readers are forwarding the same AIoT DO-A traffic from the same AIoT device by verifying the AIoT device ID, timestamp, and AIoT reader ID. This helps avoid sending the same traffic to the network multiple times unnecessarily.

NOTE: Energy, Active Time and reader selection aspects depend on RAN WGs.

6. In the RRC response message, the NG-RAN optionally includes the information indicating whether the AIoT reader is selected for the subsequent communications or not. Based on this indication, the AIoT reader can determine whether to keep forwarding the DO-A traffic from the same AIoT device. If it determines not to continue, it shall no longer forward any traffic received from the same A-IoT device for the same AIoT session. The selected AIoT reader locally stores the AIoT device context information including the Active Time.

7. The NG-RAN forwards the AIoT device ID, timestamp and the message carrying the AIoT NAS message to the AMF over the N2 UL message, and the AMF subsequently forwards the received AIoT NAS message to the responsible AIOTF over the SBI interface.

8. The AIOTF verifies if an AIoT device context exists for the device identified by the AIoT device ID. If absent, it retrieves the AIoT device permanent ID and requests the ADM for the device profile data using this ID. Upon obtaining the profile data, the AIOTF authorizes the device to send DO-A traffic to the requested AF by matching the AF ID in the AIoT NAS message with those in the profile data. If duplicate data from the same device is received, the AIOTF retains only one instance based on the timestamp. It then allocates an AIoT session ID for future communications and updates the device context data as necessary.

9. Based on the AIoT device profile data, the AIOTF determines which NEF to forward the AIoT DO-A traffic to and forwards it, including the AIoT device ID, data, and AF ID.

10. The NEF forwards the received traffic to the requested AF, including the AIoT device ID and data.

11. In response to the message in step 7, the AIOTF sends an message carrying the AIoT device AIoT device ID and the AIoT NAS message over the N2 DL message. The AIoT NAS message contains the allocated session ID.

12. The NG-RAN forwards the message to the AIoT reader selected in step 5 over RRC.

13. The AIoT reader provides the DO-A response message to the AIoT device, including the received AIoT NAS message. The AIoT reader provides energy separately or together with the response message if the Active Time stored in the AIoT device context information is shorter than the time required to send the response and the network needs further messages from the AIoT device.

14. When the AIoT device wants to send additional data to the same AF it previously sent data to, the AIoT device includes the allocated session ID in the AIoT NAS message. This message is forwarded to the AIOTF using the same mechanisms explained in steps 4 to 7.

15. When the session ID is included in the AIoT NAS message and is valid, the AIOTF may skip the authorization checking and NEF discovery processes.

16. The AIOTF directly issues the notification message towards the known NEF.

17. The NEF forwards the received traffic to the requested AF, including the AIoT device ID and data.

### 6.1.3 Impacts on Services, Entities and Interfaces

AIoT Device:

- Energy Management: The AIoT device autonomously initiates communication based on its energy harvesting capabilities.

- Timestamp support: The AIoT device provides time information indicating when the DO-A message was sent.

AIoT Reader:

- The AIoT reader forwards DO-A messages.

- It may provide energy to AIoT devices if needed.

- The reader manages session continuity based on network indications.

AIOTF:

- The AIOTF performs authorization checks to ensure devices are permitted to send DO-A traffic to specific AFs.

- Allocation of session IDs for subsequent communications streamlines the process and reduces overhead for repeated authorizations.

- Timestamp verification helps manage duplicate data.

ADM:

- The ADM maintains detailed device profiles, including registration status and access permissions.

- Efficient retrieval and updating of device profiles are necessary to support the proposed procedures.

NG-RAN:

- The NG-RAN may need to implement mechanisms for selecting AIoT readers based on traffic patterns and device context.

## 6.2 Solution #2: AIoT services support for DO-A capable AIoT Devices

### 6.2.0 High-level Solution Principles

This solution addresses Key Issue #2 "Support of DO-A Capable AIoT Devices".

The solution combines registration-like procedure and data transfer procedure, and is based on the following general principles to support AIoT services for DO-A capable AIoT Devices:

- The DO-A capable AIoT Device initiates registration-like procedure autonomously when it has pending data to be sent to the network.

- After registration-like procedure, the AIOTF uses the Command Procedure as defined in TS 23.369 [3] to read the AIoT data from the AIoT Device and sends the AIoT data to the AF via the NEF.

### 6.2.1 Description

This solution is applicable to both the Direct Connectivity and the Indirect Connectivity architectures as defined in TS 23.369 [3].

For a DO-A (Device-originated - autonomous) capable AIoT Device, the device originated traffic is triggered by the AIoT Device itself for, e.g. sending data to the network.

The principles of this solution are as follows:

- When a DO-A capable AIoT Device has pending data to be sent to the network, the AIoT Device sends Registration Request to the AIOTF.

- The AIOTF authorizes and authenticates the AIoT Device and sends Registration Accept to the AIoT Device.

- The AIOTF uses the Command Procedure as defined in TS 23.369 [3] to read the AIoT data from the AIoT Device.

- The AIOTF sends the AIoT data received from the AIoT Device to the AF via the NEF.

### 6.2.2 Procedures

Figure 6.2.2-1 describes the DO-A Procedure.



Figure 6.2.2-1: DO-A Procedure

0. AIoT Device obtains radio resource for D2R message.

Editor's note: How AIoT Device obtains radio resource for D2R message is FFS and is to be decided by RAN WGs.

1. The AIoT Device sends the AS D2R message (Registration Request) to the NG-RAN. The AS D2R message includes the AIOTF selection information including PLMN ID and/or NID and/or Third Party ID which is used by the NG-RAN to select the AIOTF. The Registration Request message is an AIoT NAS message and includes the AIoT Device ID and the Pending data indication indicating there is pending AIoT data in the AIoT Device.

NOTE 1: The AS layer message in this step and the following steps are to be defined by RAN WGs.

2. The NG-RAN selects the AIOTF based on the AIOTF selection information received in step 1.

Editor's note: Further details on AIOTF selection is FFS.

3. The NG-RAN sends the Uplink AIoT information message (Registration Request) to the AIOTF directly or via an AMF.

4. The AITOF performs Authorization and authentication procedure for the AIoT Device.

NOTE 2: Security aspects are to be defined by SA WG3.

5. The AIOTF sends the Downlink AIoT information message (Registration Accept, AIOTF AIoT Device NGAP ID) to the NG-RAN directly or via the AMF.

6. The NG-RAN sends the AS R2D message (Registration Accept) to the AIoT Device. The Registration Accept message is an AIoT NAS message.

7. Based on the Pending data indication received, the AIOTF sends the Command Request message (NAS Command Request, AIOTF AIoT Device NGAP ID, Size of the Command Response message) to the NG-RAN directly or via the AMF. The NAS Command Request is Read Request. The AIOTF AIoT Device NGAP ID is used by the NG-RAN to determine the AIoT device context in NG-RAN.

Editor's note: Other triggers for the Command Request are FFS.

Editor's note: How AIOTF derives the parameters included in the NAS Command Request is FFS.

Editor's note: Whether Registration Accept and NAS Command Request are separate or can be combined is FFS.

8. The NG-RAN sends the AS R2D message (NAS Command Request) to the AIoT Device.

9. The AIoT Device sends the D2R message (NAS Command Response) to the NG-RAN. The NAS Command Response is Read Response and includes the AIoT data.

10. The NG-RAN sends the Command Response message (NAS Command Response, AIOTF AIoT Device NGAP ID) to the AIOTF directly or via the AMF. The AIOTF determines the AIoT device context by the AIOTF AIoT Device NGAP ID received.

11. The AIOTF reports the AIoT data to the AF via the NEF.

Editor's note: Details on routing of AIoT data from the AIOTF to the AF via the NEF is FFS.

### 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: Support of Sensor Data Collection

### 6.3.0 High-level solution Principles

This solution addresses KI #2. It includes a Service Request from AF to 5GS, Parameter Configuration for the service, and Data Transfer for the service

### 6.3.1 Description

The solution is based on the following assumptions:

- Sensor Data Collection Service utilizes Periodic DO-A Sensor Data Collection Service from Device including AF, AIOTF, and AIoT Device. It uses Read/Write command type with the parameter Period or separate command types.

- Sensor Data Collection Service utilizes Periodic DO-A Sensor Data Transfer (Device, AIoT Reader, AIOTF).

- Sensor Data Collection Service Parameters can be pre-configured on AioT Devices or configured by AF. For example, Sensing Period and StartTime.

- The AIoT Reader maintains (Device ID and Correlation ID) context for every periodic behaviour.

### 6.3.2 Procedures

The procedure is shown in Figure 6.3.2-1. It includes Service Request from AF to 5GS, Parameter Configuration for the Service, and Data Transfer for the Service.



Figure 6.3.2-1: Sensor Data Collection Procedure

1. Step 1 to step 6 of Procedure for Command in clause 6.2.3 of TS 23.369 [3] with additional parameters. AF sends AIoT Command Request to NEF. In includes Device(s) Info, Location (External), AF Transaction ID, Command Type Read, Sensing Result Offset, Length, Period, and Sensing Parameters ([Sensing Period Offset, Period], [StartTime Offset, Now/time/Off]). Sensing Parameters are optional. NEF selects AIOTF, and then NEF sends AIoT Command Request to AIOTF. AIOTF checks AF Authorization by retrieving AF Authorization Profile in ADM. AIOTF sends AIoT Command Response to NEF. It includes Status (Success/Failure), Transaction ID. NEF sends AIoT Command Response to AF. It includes Status (Success/Failure), AF Transaction ID.

2. Step 7 to step 10 of Procedure for Inventory in clause 6.2.2 of TS 23.369 [3]

3. AIOTF retrieves Device Profile Data Including DO-A Capability. If the device does not support DO-A Capability, steps 15 to 19 are skipped.

4a~8a, 4b~8b. Parameter configuration with Write Command can be done instead of parameter configuration included in steps 4~8.

4. AIOTF sends AIoT Command Request to AIoT Reader. This includes Device ID (temporary), (Reader ID), Command Type Read, Correlation ID, Sensing Result Offset, Length, Period, and Sensing Parameters ([Sensing Period Offset, Period], [StartTime Offset, Now/time/Off]). AIoT Reader stores Correlation ID with AIoT Device ID as context data.

5. AIoT Reader sends AIoT Command Request to AIoT Device. This includes Device ID (temporary), (Reader ID), Command Type Read, Correlation ID, Sensing Result Offset, Length, Period, and Sensing Parameters ([Sensing Period Offset, Period], [StartTime Offset, Now/time/Off]). When 4a~8a, 4b~8b are done, Sensing Parameters are omitted.

6. When AIoT Device receives Period with Command Type Read, it starts periodic Read behavior based on the Period value. When AIoT Device receives Sensing Parameters, it sets the parameters to the device.

For example, it sets Sensing Period to a specific Period, and/or sets StartTime to Now, a specific time, or Off. If StartTime is set to Now, the device reads and report Sensor Result immediately and every Period.

If StartTime is set to a specific time, then the device reads and reports Sensor Result at that time and every Period after that.

If StartTime is set to Off, the device reads and reports Sensor Result once, then stops periodic reading and transfer.

7. AIoT Device sends AIoT Command Response to AIoT Reader. This includes Device ID (temporary), and Sensing Result.

8. AIoT Reader sends AIoT Command Response to AIOTF. This includes Device ID (temporary), Sensing Result, and Correlation ID. AIoT Reader retrieves Correlation ID with AIoT Device ID from the stored context.

9. AIOTF sends AIoT Command Notify to NEF. This includes Device ID (permanent), Sensing Result, and Transaction ID. AIOTF retrieves Transaction ID with Correlation ID from the stored context.

10. NEF sends AIoT Command Notify to AF. This includes Device ID (permanent), Sensing Result, and AF Transaction ID. NEF retrieves AF Transaction ID with Transaction ID from the stored context.

11. Every Period, when the energy is enough, the device reads and reports Sensor Result. Depending on the size of the report, the radio resource allocation procedure may vary.

Editor's note: How the AIoT Device supports timer is FFS.

12. AIoT Device sends AIoT Command Report to AIoT Reader. This includes Device ID (temporary), Sensing Result.

13. AIoT Reader sends AIoT Command Report to AIOTF. This includes Device ID (temporary), Sensing Result, and Correlation ID. AIoT Reader retrieves Correlation ID with AIoT Device ID from the stored context. If the context is not stored, AIoT Reader sends AIoT Command Report with Device ID (temporary), Sensing Result, and temp-Correlation ID, which AIoT Reader generates as indication of empty Correlation ID.

14. AIOTF sends AIoT Command Notify to NEF. This includes Device ID (permanent), Sensing Result, and Transaction ID. AIOTF retrieves Transaction ID with Correlation ID from the stored context. If step 13 includes temp-Correlation ID, AIOTF retrieves Transaction ID with Device ID (temporary).

15. NEF sends AIoT Command Notify to AF. This includes Device ID (permanent), Sensing Result, AF Transaction ID. NEF retrieves AF Transaction ID with Transaction ID from the stored context.

### 6.3.3 Impacts on services, entities and interfaces

Impacts on existing entities:

AIOTF:

- Receives AIoT Command Request for Sensor Data Collection Service from AF through NEF.

- Performs Inventory procedure and then sends Read Command Request with Period and Sensing Parameters.

- Performs Inventory procedure and then sends Write Command Request with Sensing Parameters.

- Retrieves Device Profile Data including DO-A Capability. If the device does not support DO-A Capability, AIOTF skips DO-A related steps.

- Receives AIoT Command Report from Device(s) through AIoT Reader(s) and delivers it to the AF through the NEF.

- Sends AIoT Command Notify to AF via NEF.

ADM:

- Supports the AIoT Device profile, including DO-A Capability.

AIoT Reader:

- Supports the AIoT TempID handling, including Device ID and Correlation ID mapping, and maintains the mapping context.

- Supports DO-A procedure for AIoT Command Report from AIoT Device(s).

AIoT Device:

- Supports DO-A procedure for AIoT Command Report from AIoT Device.

- Reads and reports Sensing Data to AIoT Reader periodically via the DO-A procedure.

- Supports timer.

- Considers energy status for its behaviour.

- Sets Sensing Parameters and behave according to the Sensing Parameters.

- Performs radio resource allocation procedure depending on the size of the report.

## 6.4 Solution #4: Architecture enhancements to support DO-A capable devices

### 6.4.0 High-level solution Principles

This solution proposes call flows to support registration and handling of DO-A capable devices. The solution builds upon an AF request that is to be carried out more than once. The core network uses legacy inventory procedure to find Ambient IoT devices. The Ambient IoT devices indicates their support for registration in the inventory response. The core network registers the device and after that keeps the path back to AF alive.

In addition, a UE capability like procedure is provided so that the core network can ask each device for supported features.

### 6.4.1 Description

The Ambient IoT devices of type 2b/c may be able to initiate communication independently with the help of DO-A traffic. This solution builds on the principle that the Ambient IoT device indicates support for registration in response to an AIoT paging message. The support for registration may also be seen as an indication for support of DO-A communication.

Registration like procedure is proposed, to ensure the operator can properly control which devices are allowed to send data in the licensed spectrum owned by the operator.

The solution does not take a stance on whether the reader prefers to use regular paging or activate DO-A resources for the Ambient IoT device.

Further the solution proposes a complementary procedure allowing the network to ask the Ambient IoT device for supported features. This may be helpful if Ambient IoT devices are to support many features and/or if the Ambient IoT device subscription on network side is minimalistic. Another aspect being considered is that features may not always be available, if the battery is low, DO-A communication may not be possible, the device may not have enough power to use an attached sensor etc.

### 6.4.2 Procedures

#### 6.4.2.1 Ambient IoT device registration and DO-A execution



Figure 6.4.2.1-1: Ambient IoT device registration and DO-A execution

1. The AF sends Nnef\_AIoT\_Inventory/Command Request (DO-A dependent service request) to the NEF with a service request that is dependent on DO-A. For example, regular reporting of temperature, etc.

2. NEF selects AIOTF as specified in TS 23.369 [3].

3. Naiotf\_AIOT\_Inventory/Command request (DO-A dependent service request) is sent to the selected AIOTF.

4. The AIOTF determines registration is required based on the service being DO-A dependent.

5. AIOTF sends NGAP Inventory Request message (Inventory request transfer (A-IoT Device Identification Requested, Follow on Command Indication)) to the reader.

6. NGAP Inventory Response ().

7. AIoT paging occurs.

8. Ambient IoT NAS Inventory Response message (Registration capability indication, Ambient IoT device ID) is sent to the reader from the Ambient IoT device. The registration capability indication is used to indicate to the network this device is capable of registration. It may also be seen as an implicit indication the Ambient IoT device support DO-A communication.

Editor's note: Whether security is required to protect the registration capability indication is FFS.

9. NGAP Inventory Report message (Inventory Report Transfer (Ambient IoT NAS Inventory Response message (Registration capability indication, Ambient IoT device ID), RAN A-IoT Device NGAP ID) is sent from reader to AIOTF.

10. Based on receiving the registration capability indication, the AIOTF determines to attempt registering the Ambient IoT device.

11. The AIOTF sends Nadm\_Registration request message (Ambient IoT device ID, AIOTF ID) to the ADM.

12. The ADM determines Ambient IoT device is authorized to register with the network. For example, this can be based on subscription data.

13. Upon successful authorization, the ADM register the AIOTF ID for the Ambient IoT device in the ADM.

14. The ADM sends Nadm\_Registration response message (Ambient IoT device ID, result) to the AIOTF, providing the result of the registration attempt.

15. The AIOTF sends NGAP Command Request message (Command request transfer(RAN A-IoT Device NGAP ID, Keep context indication, A-IoT NAS PDU (Command (Registration accept)))) to the reader. Keep context indication is used as an expansion of follow on command indication. Since the DO-A communication may occur over a long time, the reader needs to be able to route DO-A communication over potentially a long time.

16. The reader sends Reader 2 device message (A-IoT NAS PDU (Registration accept)) to the Ambient IoT device.

17. The AIOTF sends NGAP Command Request message (Command request transfer (RAN A-IoT Device NGAP ID, DO-A service indication, A-IoT NAS PDU (DO-A dependent service request payload))) to the reader. The DO-A service indication may be used by the reader to determine whether to activate DO-A or do regular paging for the DO-A service.

18. Execute the DO-A dependent service request. How the reader and Ambient IoT device configures is out of scope for this solution. After this, the Ambient IoT device can send data autonomously.

Editor's note: Data delivery details are FFS.

Editor's note: RAN working group coordination is required to determine context storage aspects in gNB.

#### 6.4.2.2 AIoT device capability syncronization

Editor’s note: It is FFS whether this procedure is needed.



Figure 6.4.2.2-1: AIoT device capability synchronization

1. The AIOTF sends NGAP Command Request message (Command request transfer (RAN A-IoT Device NGAP ID, first A-IoT NAS PDU (Command (AIoT device capability request indication)))) to the reader. The AIOT device capability request indication in the command is used by the Ambient IoT device to determine to send AIoT device capability container information element.

2. The reader sends Reader 2 device message (first A-IoT NAS PDU (AIoT device capability request indication)))) to the Ambient IoT device.

3. The Ambient IoT device sends Device to reader message (second A-IoT NAS PDU (AIoT device capability container information element) to the reader. The AIoT device capability container information element can indicate support for DO-A, power saving features, security capabilities, available sensor(s) etc.

4. The reader sends NGAP Command response message (Command Response Transfer (AIoT device capability container information element), RAN A-IoT Device NGAP ID) to the AIOTF.

5. The AIOTF sends Nadm\_DM\_Update Request (Ambient IoT device ID, AIoT device capabilities) to the ADM with the purpose of registering the AIoT device capabilities with the subscription data of the Ambient IoT device.

6. The ADM sends Nadm\_DM\_Update Response (result) to the AIOTF.

### 6.4.3 Impacts on Services, Entities and Interfaces

AIOTF:

- Support registration of AIoT devices.

- Support AIoT capabilities.

Reader:

- Context handling for DO-A devices.

ADM:

- Registration.

- AIOT device capabilities.

AIoT device:

- Registration.

- AIOT device capabilities.

- DO-A.

## 6.5 Solution #5: DO-A procedure with configured routing information

### 6.5.0 High-level solution Principles

This solution aims to resolve KI#2 to support DO-A Capable AIoT Devices, the following principles are followed in this solution:

- This solution has reused the architecture defined in clause 4.2.2 in TS 23.369 [3]. This solution is applied to both direct connectivity and indirect connectivity for Topology 1.

- The AIoT Device is not required to perform the registration procedure first before sending the DO-A data.

- AIoT Device sends the DO-A routing information along with the DO-A message for AIOTF to find the proper AF.

- AF subscribes to the DO-A Data notify by sending a Subscribe Request to the AIOTF (optionally via the NEF).

- AIOTF derives the corresponding AF according to the routing information in the NAS DO-A Data Transfer Request message and the context generated in DO-A data subscribe procedure.

### 6.5.1 Description

This solution resolves KI#2 for support of DO-A Capable AIoT Devices.

This solution has the following assumptions:

1) AIoT Device is pre-configured or configured by the network with DO-A routing information.

2) AIoT Device sends the DO-A routing information along with the DO-A message for AIOTF to find the proper AF.

3) The NG-RAN selects the correlated AIOTF according to AIOTF information in the temp ID if a temp ID is included in the D2R AS message.

4) AF subscribes to the DO-A Data notify by sending a Subscribe Request to the AIOTF (optionally via the NEF). AIOTF updates AIoT DO-A Profile in ADM with the associated AF subscription.

5) AIOTF receiving the DO-A data can query the ADM to find the DO-A data associated AIOTF(s) and forward the received DO-A data to the associated AIOTF(s).

6) AIOTF derives the corresponding AF according to the routing information in the NAS DO-A Data Transfer Request message and the associated (AF) Transaction ID used in DO-A data subscribe procedure.

### 6.5.2 Procedures

#### 6.5.2.1 DO-A data subscribe procedure



Figure 6.5.2-1: Figure for DO-A data subscribe procedure

1. The AF sends the DO-A data subscribe request to NEF with AF ID and target AIoT device information to subscribe for the notification of the DoA data.

2. NEF performs AIOTF selection based on the target AIoT device information.

3. The NEF sends the DO-A data subscribe request to the selected AIOTF with a Transaction ID.

4. The AIOTF authorizes the AF request to check whether the AF is allowed to subscribe to DO-A delivery, based on the AF authorization data stored in the ADM.

5. If authorization succeeded, the AIOTF updates AIoT DO-A Profile in ADM with the associated AF subscription.

6. If the AIOT device is not pre-configured, the AIOTF allocates the routing information for the DO-A data transfer and configure the AIOT device via e.g. AIoT Command procedure defined in clause 6.2.2 in TS 23.369 [3]. In this step, the AIOTF may also allocate a Temp ID to AIoT Device for NAS DOA Data Transfer.

7. AIOTF sends response to the NEF with a Transaction ID for the DO-A data subscribe request.

8. NEF sends response to AF with AF Transaction ID for the DO-A data subscribe request.

#### 6.5.2.2 DO-A data transfer procedure



Figure 6.5.2-2: Procedure for DO-A procedure with configured routing information

0. DoA routing information (e.g. AF ID or AIOTF allocated DO-A association ID) at the AIoT device side or configured by the network as defined in clause 6.5.2.1. Security information for DO-A traffic may also be pre-configured or configured along with the DoA routing information.

Editor’s note: DO-A traffic security mechanism will be determined by SA WG3.

1. The AIoT Device decides to trigger a DO-A message (e.g. detecting DO-A trigger broadcast signal, etc.).

Editor's note: DO-A trigger broadcast signal is further defined in RAN WGs.

2. The AIoT Device sends the AS D2R message (Temp ID, NAS DOA Data Transfer Request message (DO-A data, AIoT device ID, routing information)) to the NG-RAN. AIoT device ID may be a permanent Device ID or Temp Device ID. The temp ID is also provided in the AS D2R message if the AIOTF has allocated a Temp ID to AIoT Device during or after the Command procedure, or during the previous DO-A Data Transfer procedure.

3. The NG-RAN allocates an NGAP ID for the AIoT device and forwards the NAS DO-A Data Transfer Request message in Initial DO-A message to the AIOTF. If a temp ID is included AS D2R message, the NG-RAN can select the AIOTF according to the temp ID. If the temp ID is not included in AS D2R message or the AIOTF derived from the AIOTF in the temp ID can not be selected, the NG-RAN can select an AIOTF which can serve the AIoT Device. The selected AIOTF can query the ADM to find the DO-A data associated AIOTF(s) and forward the received DO-A data to the associated AIOTF(s)

Editor’s note: Whether and how temp ID can be used to find the AIOTF is FFS.

4. Upon receiving the Initial DO-A Message, the AIOTF performs a device check with device profile data retrieved from the ADM to validate the AIoT device.

Editor's note: Details for device check for DO-A Data Transfer procedure will be determined by SA WG3.

5. After the successful device check, the AIOTF derives the corresponding AF according to the routing information in the NAS DO-A Data Transfer Request message and the associated Transaction ID received in step 3 of clause 6.5.2.1. The AIOTF sends the Naiotf\_AIoT\_Data Transfer message including the DO-A data and AIoT Device ID to the NEF.

6. The NEF invokes the AIoT\_Data Transfer service to forward the DO-A data to the AF according to the AF Transaction ID and AF ID used in DO-A data subscribe procedure.

7. The AF sends the AIoT\_Data Transfer\_Response to NEF with AIoT device ID and the response to the DoA data, which may include further data or acknowledgments related to the DO-A Data Transfer process.

8. The NEF invokes AIoT\_Data Transfer\_Response to AIOTF. The message includes the DO-A data response and related AIoT device ID.

9. The AIOTF allocates an NGAP ID for the AIoT device and sends DL NAS message to NG-RAN with the DO-A data response. In this step, the AIOTF may also allocate a Temp ID to AIoT Device NAS DOA Data Transfer Response message.

Editor’s note: Whether inventory procedure for the DL NAS messages transfer is needed is FFS.

10. The NG-RAN sends the AS R2D message to the AIoT device including the NAS message.

### 6.5.3 Impacts on services, entities and interfaces

The solution has impacts on the following entities:

AIoT Device:

- Support to initiate DO-A message transfer procedure and send routing information along with the DO-A data.

AIOTF:

- Support to route the DO-A message to proper NEF/AF according to the routing information.

NG-RAN:

- Support to select the AIOTF based on the temp ID if provided by the AIoT device.

- Support to establish NGAP connection with AIOTF for DO-A message transfer.

## 6.6 Solution #6: Support Reporting operator triggered by events without registration for DO-A capable AIoT Devices

### 6.6.0 High-level Solution Principles

This solution addresses Key Issue #2 "Support of DO-A Capable AIoT Devices".

AIoT device sends report message when triggered by events, includes pending data, power on, device specific events (e.g., temperature higher than a threshold). The information for the device specific events can be provisioned by AF via Command operation, e.g., writing the threshold to the AIoT device.

### 6.6.1 Description

This solution is applicable to both the Direct Connectivity and the Indirect Connectivity architectures as defined in TS 23.369 [3].

For a DO-A capable AIoT Device, the device is triggered by events to report its presence and/or send data to the network.

The principles of this solution are as follows:

- No registration-like procedure needed for the DO-A capable AIoT Device.

- The AIOTF for routing the DO-A report and the AIOTF for inventory and command operations can be different.

- The events triggered DO-A report includes target AF and may include data from the AIoT Device.

### 6.6.2 Procedures

Figure 6.6.2-1 describes the Reporting procedure from DO-A capable AIoT Device.



**Figure 6.6.2-1: DO-A device reporting procedure**

0. The AIoT device is pre-configured with target AF information, e.g., FQDN, by the owner of the AIoT device for routing the information in the Report Request. Allowed AF(s) may be pre-configured in the AIoT device profile data in ADM. The information for device specific events may be provisioned by the AF using the Command operation, e.g., write a sharehold related to a device specific event to the AIoT device.

NOTE 1: The allowed AF(s) in the ADM can be changed via OAM. The target AF information may be configured by the owner of the device via Inventory and Command operator.

1. The AF subscribes to the NEF with the AF information and optional the service area. The NEF selects AIOTF(s), e.g., based on pre-configuration or the service area, and subscribes to the selected AIOTF(s).

NOTE 2: It is assumed all the AIOTFs serving the service area and/or serving the AF are subscribed by the NEF.

2. The AIoT device is triggered by events, e.g., pending data, power on, or device specific events.

3. The AIoT device sends D2R message including AIoT NAS Report Request (Device ID, target AF, [data]) to the RAN Reader. In case there are pending data in the AIoT device, the data is included in the AIoT NAS Report Request message.

Editor's note: How the AIoT device sends the D2R message to the RAN Reader is FFS.

Editor's note: Whether the solution is applicable for UE Reader case is FFS.

NOTE 3: Security aspects related to the Device ID and the data protection are to be defined by SA WG3.

4. The NG-RAN selects an AIoTF, e.g., based on local policy or pre-configuration.

5. The NG-RAN sends a N2 request message (indirect) or AIOT2 request message (direct) including the Reader ID and the AIOT NAS Report Request message towards the selected AIOTF.

6. The AIOTF requests authorization data from ADM.

7. The AIOTF authorizes the Report Request from the device, e.g., based on whether the target AF is in the allowed AF(s) per the device, per the group of the device, or per the network, whether the device is allowed to initiate Report Request, whether the location is allowed to send the report per the device, etc. If the authorization of report from the AIoT device is successful, goes to step 8, otherwise goes to step 9 with proper cuase value.

8. The AIOTF maps the Reader ID into location information, and sends a Notify (Device ID, location info, [data]) message towards the AF via the NEF based on the target AF. The NEF forwards the Notify message towards the AF.

9. The AIOTF responds to the RAN Reader.

The AIOTF may update the last known reader information in the AIoT device profile data in the ADM.

10. The RAN Reader sends R2D message to the AIoT Device.

### 6.6.3 Impacts on Services, Entities and Interfaces

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

**AIoT Device:**

- Support initiate Report Request procedure triggered by events.

**NG-RAN:**

- Support AIOTF selection.

**AIOTF:**

- Support Report Request authorization.

- Support sending Device ID, location information, and optional data to target AF indicated in the Report Request.

**NEF:**

- Support managing AF sessions for AIOT service between AFs and AIOTFs.

**ADM:**

- Support providing authorization data to AIOTF when requested.

## 6.7 Solution #7: DO-A procedure for DO-A Capable AIoT Devices

### 6.7.0 High-level solution Principles

This solution is for Key Issue #2, corresponding to bullet 3: How an AIoT Device sends data to the AIOTF autonomously. It includes DO-A procedure to send data to the AIOTF, get network resource/assistance information to initial DO-A procedure, and DO-A policy information which describe when will perform the DO-A procedure.

### 6.7.1 Description

This solution is for Key Issue #2, corresponding to bullet 3: How an AIoT Device sends data to the AIOTF autonomously.

This solution is to support for an DO-A Capable AIoT Device autonomously originated DO-A procedure to send data to the AIOTF, and support for routing the received data by AIOTF to AF.

The main points are as following:

- The DO-A Capable AIoT Devices support autonomously originat DO-A procedure to send data to the AIOTF.

- The DO-A Capable AIoT Device has pre-configurated network resource/assistance information(e.g. frequency, Qos, Resource Expiration Date, etc) for autonomously originating DO-A procedure; or support to receive the network resource information/assistance information (e.g. frequency, Qos, Resource Expiration Date, etc) from the network for autonomously originating DO-A procedure, using by AIoT write commands or new AIoT service, or network system information etc.

NOTE 1: How to get and the details of the network resource/assistance information for autonomously originating DO-A procedure will be coordinated with RAN WG2.

- When the DO-A Capable AIoT Device will autonomously originats DO-A procedure to send data, is based on the DO-A policy information. The DO-A policy information may be received from network or AF via the network, which send by AF using AIoT write commands or some new AIoT service. Or the DO-A policy information can be pre-configurated in the AIoT device or UICC if have.

- The DO-A policy information may include:

- Target information: identify where and which AF the DOA data sends/routes to by AIoT device, for example AF identify, etc；

- Service policy: describe when and how the AIot device autonomously originated to send DOA datas, such as: 9:00 am every day, when the timer expired, the upper layer initials, etc.

NOTE 2: The details of DO-A policy are coordinated between the operator and AF vender, which is out of 3GPP scope.

- The DO-A Capable AIoT Device supports to autonomously originating procedure to send data to the AIOTF, and support for routing the received data by AIOTF. The procedure may include: security data, target information and the data information. The security data is used for the network authentication AIoT device; and the target information is used to identify where and which AF the DOA data sends/routes to, for example AF identify, etc; the data information is the real data which the AIoT device wants to send for AF.

### 6.7.2 Procedures

The following figure presents a DO-A procedure for DO-A Capable AIoT Devices for Topology 1 and Topology 2.

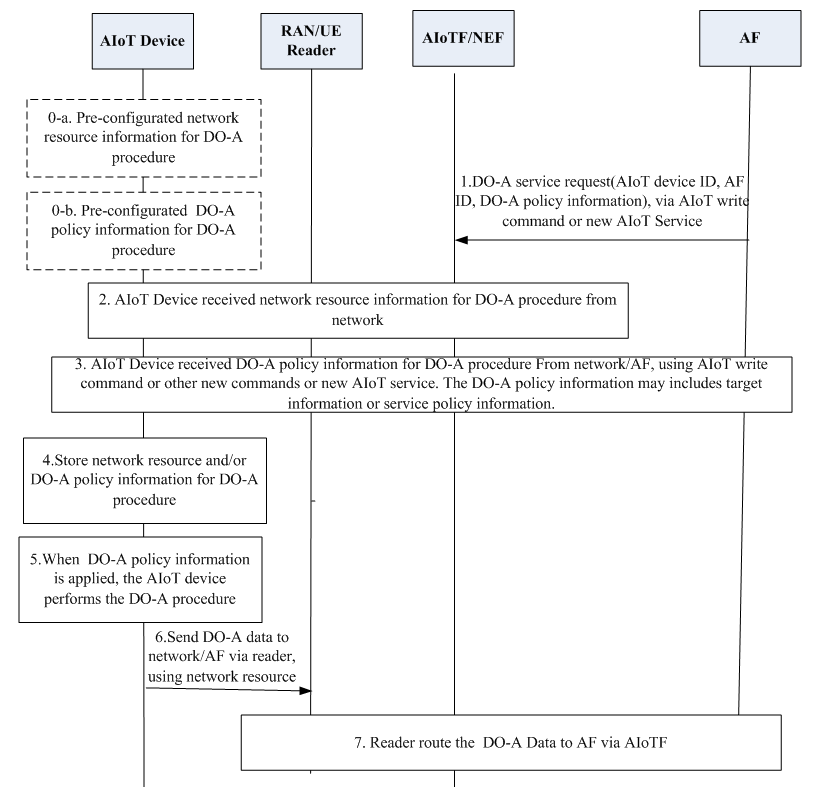


Figure 6.7.2-1: DO-A procedure for DO-A Capable AIoT Devices

0-a. DO-A Capable AIoT Devices may be pre-configured with network resource/assistance information(e.g. frequency, QoS, Resource Expiration Date, etc) for autonomously originating DO-A procedure.

0-b. DO-A Capable AIoT Devices may be pre-configured with DO-A policy information for autonomously originating DO-A procedure.

NOTE 1: How information is configured into AIoT device is out of scope of 3GPP.

NOTE 2: How to get and the details of the network resource/assistance information for autonomously originating DO-A procedure will be coordinated with RAN WG2.

1. AF sends like DO-A service request to NEF via AIoT write command or new AIoT Service, it may includes following parameters: AIoT devices ID, AF ID, DO-A policy information, and so on.

- DO-A policy information may include:

- Target information: identify where and which AF the DOA data sends/routes to by AIoT device, for example AF identify, etc；

- Service policy: describe when and how the AIoT device autonomously originated to send DOA data, such as: 9:00 am every day, when the timer expired, the upper layer initials, etc.

NOTE 3: The details of DO-A policy are coordinated between the operator and AF vender, which is out of 3GPP.

2. AIOTF/NEF receives the DO-A service request from AF, and will check the authorization of AF and the authorization of DO-A Capable of AIoT devices based on the subscription in ADM. If it is allowed, the network function(e.g. AIOTF or RAN/UE reader) will send the network resource information/assistance information(e.g. frequency, QoS, Resource Expiration Date, etc) for DO-A Capable of AIoT devices autonomously originating DO-A procedure. DO-A Capable of AIoT devices receives these network resource information/assistance information.

3. AIOTF/NEF sends the DO-A policy information from AF to DO-A Capable of AIoT devices. DO-A Capable of AIoT devices receives these DO-A policy information.

4. DO-A Capable of AIoT devices store these receiving network resource and/or DO-A policy information for DO-A procedure from network.

5. When DO-A policy information is applied, for example: the timers from the DO-A policy information expired, the DO-A Capable of AIoT device performs the DO-A procedure.

6. The DO-A Capable of AIoT device sends DO-A data to network/AF via RAN/UE Reader, using the storing or pre-configured network resource. The procedure may include: security data, target information and the data information. The security data is used for the network authentication AIoT device; and the target information is used to identify where and which AF the DOA data sends/routes to, for example AF identify, etc; the data information is the real data which the AIoT device wants to send for AF.

7. RAN/UE Reader routes the DO-A Data from AIoT device to AF via AIOTF based on the target information provided by AIoT device or other solutions.

Editor’s note: How the RAN/UE Reader routes the DO-A Data to AF will be coordinated with solutions for KI 2 bullet of “Support for routing the data received by AIOTF from an AIoT Device to an AF”, or be FFS.

### 6.7.3 Impacts on services, entities and interfaces

NEF:

- Supports AF to provide DO-A policy information;

AIOTF:

- Supports to receive DO-A data from DO-A capable AIoT Device and route for AF;

- Supports to provide network resource/assistance information(e.g. frequency, Resource Expiration Date, etc) for AIoT Device DO-A procedure;

RAN Reader or UE Reader:

- Supports to receive DO-A data from DO-A capable AIoT Device and route for AIOTF;

- Supports to provide network resource/assistance information(e.g. frequency, Resource Expiration Date, etc) for AIoT Device DO-A procedure；

AIoT Device：

- Pre-configured or stores network resource/assistance information(e.g. frequency, Resource Expiration Date, etc) and/or DO-A policy information;

- Performing DO-A procedure once it is needed to send DO-A data.

- Support DO-A Policy(e.g. timer)

NOTE: How the AIoT device support DO-A Policy, e.g. timer, is up to UE implementation.

## 6.8 Solution #8: Service Procedure for DO-A Capable AIoT Devices

### 6.8.0 High-level solution Principles

This solution addresses Key Issue #2 "Support of DO-A Capable AIoT Devices", especially the following aspects:

- How the AIoT Device informs the network of its presence autonomously (e.g., an AIoT Device initiated registration-like procedure) and what are the triggers for the DO-A capable device to inform the network of its presence.

- How an AIoT Device sends data to the AIOTF autonomously.

- Support for routing the data received by AIOTF from an AIoT Device to an AF.

The solution defines two types of DO-A messages sent from the AIoT Device: one is initiating message which is used to determine the serving AIOTF for the AIoT Device; another is DO-A data transfer message which is used to transfer AIoT data from the AIoT Device to the AF through the core network.

This solution also proposes call flows for initiating message and DO-A data transfer message. In addition, an AF subscription procedure is provided so that the AF can subscribe the AIoT data from a specific AIOT Device.

### 6.8.1 Description

The Ambient IoT devices of type 2b/c may initiate communication independently with DO-A traffic. This solution is applicable to both the Direct Connectivity and the Indirect Connectivity architectures for Topology 1.

The principles of this solution are as follows:

- Two types of DO-A messages sent from the AIoT Device: one is initiating message which is used to determine the serving AIOTF for the AIoT Device; another is DO-A data transfer message which is used to transfer AIoT data from the AIoT Device.

- The procedure for initiating message to determine the serving AIOTF for the AIoT Device is proposed.

- The procedure for DO-A data transfer frjom the AIoT Device is proposed.

- The procedure for AF subscription for the AIoT data from a specific AIoT Device is proposed.

- The ADM is used to store the serving AIOTF for the AIoT Device and the subscription relationship between the AIoT Device and the AF.

- The AIOTF stores the subscription relationship between the AIoT Device and the AF and sends the AIoT data received from the AIoT Device to the AF via the NEF.

### 6.8.2 Procedures

#### 6.8.2.1 Initiating message and data transfer procedure



Figure 6.8.2.1-1: Initiating message and data transfer procedure

0. The AIoT Device decides to trigger an initiating message based on some conditions, e.g. the AIoT Device needs to report AIoT data such as sensing data detected, the time for periodic reporting arrives, or the AIoT Device moves to a new position. In this stage the AIoT Device has no serving AIOTF available.

Editor’s note: Whether using registration like procedure instead of this initiating message procedure is FFS.

1. The AIoT Device sends the initiating message to the NG-RAN. The initiating message includes the AIoT Device ID information, optional pending data transfer indication.

2. The NG-RAN selects the serving AIOTF for the AIoT Device, taking into account the Device ID information, the PLMN ID and NID, and/or the AIoT area which this AIoT Device belongs to.

3. The NG-RAN sends the initiating message to the selected AIOTF directly (for direct connectivity option) or via an AMF (for indirect connectivity option); the initiating message includes the AIoT Device ID information.

4. The AIOTF discovers the serving ADM and interacts with the ADM to fetch the subscription information and may update the AIoT Device information stored in the ADM.

5. The ADM updates the AIoT Device information and the Device’s serving AIOTF information.

6. The AIOTF sends the initiating message response with the serving AIOTF ID to the NG-RAN directly or via the AMF.

Editor’s note: The details of AIoT Device or Temporary ID used in the initiating request/response message is FFS.

7. The NG-RAN sends the initiating message response with the serving AIOTF ID to the AIoT Device. The AIoT Device stores the serving AIOTF ID

8. The AIoT Device decides to trigger an AIoT data transfer message when the AIoT Device needs to report AIoT data such as sensing data detected, or the time for periodic reporting arrives.

9. The AIoT Device sends the data transfer message to the NG-RAN. The data transfer message includes the AIoT Device ID information, the AIoT data, and its serving AIOTF ID.

10. The NG-RAN sends the data transfer message to the indicated AIOTF.

11. The AIOTF sends the data transfer message response to the AIoT Device through NG-RAN.

12. The AIOTF finds the AF subscribing to the AIoT data of the AIoT Device, and then transmits the data transfer message to the NEF which serves the AF. The AF subscribing procedure is described in clause 6.8.2.2.

NOTE: The ADM may store the information of the subscription relationship between an AF and the AIoT Device; in this case, the AIOTF interacts with the ADM to fetch this subscription information.

13. The NEF transmits the data transfer message to the AF.

14. The AF may send back the data transfer message response to the AIOTF through the NEF.

#### 6.8.2.2 AF subscription procedure



Figure 6.8.2.2-1: AF subscription procedure

1. If an AF decides to subscribe the AIoT data from a specific AIoT Device, the AF sends a subscription request to the NEF. The subscription request includes the AIoT Device ID, AF ID.

2. The NEF discovers an ADM based on the AIoT Device ID and interacts with the selected ADM to fetch the serving AIOTF for this AIoT Device.

NOTE: The ADM may store the information of the subscription relationship between the AF and the AIoT Device.

3. The NEF transmits the subscription request to the AIOTF serving the AIoT Device. The subscription request includes the AIoT Device ID, AF ID.

4. The AIOTF stores the information of the subscription relationship between the AF and the AIoT Device.

5. The AIOTF sends the subscription response to the NEF to indicate the subscription request successes or fails.

6. The NEF transmits the subscription response the AF.

### 6.8.3 Impacts on Services, Entities and Interfaces

AIOTF:

- Handle the AIoT data of AIoT Devices.

- Interact with the ADM to store the AIoT Device information.

- Store the subscription information.

NG-RAN:

- Select the AIoTF serving the AIoT Device.

- Route the messages between the AIoT Device and the AIOTF.

ADM:

- Store the AIoT Device information.

- Optionally store the subscription information.

AIoT Device:

- Send DO-A initiating messages.

- Send DO-A data transfer messages.

NEF:

- Route the messages between the AF and the AIOTF

## 6.9 Solution #9: Autonomous registration and data transfer from AIoT Device

### 6.9.0 High-level solution Principles

The following principles apply:

- The Reader broadcasts system information that defines contention-based uplink resources for initial access of AIoT Device.

- An AIoT Device, upon power-on or sensing an event to report, uses the broadcasted information to autonomously register and once registered to the network, it can transmit data to the AF via the network.

- The AIOTF is enhanced to support the AF request for the DO-A activation, handle registration and data transfer request from the DO-A capable AIoT Device forwarded by the Reader, authenticate and authorize the request, create device context, respond to the AIoT Device with the assigned temporary ID.

Editor’s note: The need for the request from AIOTF to the NG-RAN for broadcasting access parameters is FFS.

### 6.9.1 Description

This solution addresses Key Issues #2 by defining the procedure for the DO-A capable AIoT Device applicable to both Topology 1 (using RAN Readers) and Topology 2 (using UE Readers). It enables a DO-A capable AIoT Device to trigger its own registration with the network to autonomously inform the network of its presence without a prior network command and to send data to the designated AF based on the AF requested DO-A activation.

### 6.9.2 Procedures

The DO-A procedure can be initiated by the AF to request the activation for one or more DO-A capable AIoT Devices or a group of DO-A capable AIoT Devices in an area to execute the autonomous registration and data transfer.

The DO-A procedure can be also activated based on configuration in the network. In this case, the AIOTF is configured with information to select NG-RAN node(s) and optionally Readers and send DO-A activation request.

#### 6.9.2.1 DO-A procedure for Topology 1



Figure 6.9.2.1-1: Device initiated Registration and Data Transfer procedure for Topology 1

1. The AF requests for the AIoT DO-A activation which may include the External Target Area information and/or information about the target AIoT Device(s) to the NEF.

Editor’s note: How to handle and coordinate the requests from multiple AFs is FFS.

2. The NEF selects the AIOTF(s) as described in clause 5.3.1 of TS 23.369 [3] and sends the AIoT DO-A activation request from the AF to the selected AIOTF(s).

3. The AIOTF selects NG-RAN node(s) and optionally RAN readers based on the configured NG-RAN node selection information. The AIOTF may also consider the Target Area information and/or information about the target AIoT Device(s) if received in Step 1, and the stored last known RAN Reader information if available e.g. by means of prior Inventory procedure.

4. The AIOTF sends the AIoT DO-A activation response to the AF via NEF.

5. The AIOTF sends the DO-A activation request to each selected NG-RAN node, either directly or through the selected AMF which may include the Requested Service Area Information and/or the AIoT Identification Information.

Editor’s note: The detailed parameters to be included in the DO-A activation request is FFS.

6. The RAN Reader periodically broadcasts access parameters related to Random Access for AIoT Device for autonomous transmissions based on the DO-A activation request from the AIOTF.

NOTE 1: The mechanism for broadcasting access parameters needs coordination with RAN WGs.

7. The AIoT Device listens to access parameters from the RAN Reader and performs Random Access to establish the AS connection with the RAN Reader.

8. The AIoT Device transmits the AIoT Registration Request message including the AIoT Device Permanent Identifier. The RAN Reader receives the request and forwards the AIoT Registration Request to the AIOTF directly or via an AMF.

Editor’s note: Whether and how the privacy protection for the AIoT Device Permanent Identifier applies is FFS.

9. The AIOTF validates the AIoT Registration Request message with DO-A capability of the AIoT Device and the target AF information in the AIoT Device Profile Data provisioned, the Target Area information and/or information about the target AIoT Device(s) configured or received in Step 1.

If validation fails, the AIOTF issues failure response to the AIoT Device and the rest of the procedure is not performed.

Upon successful, the AIOTF updates the AIoT Device Profile Data in the ADM with the Last known AIOTF information.

The AIOTF retrieves the AIoT Device Temporary ID from the ADM, associating it with the last known Reader and the target AF and stores the mapping between the RAN Reader ID, AIoT Device Temporary ID and the AF ID in the AIoT Device context.

NOTE 2: The security aspects for authentication, authorization and the use of AIoT Device Temporary ID needs coordination with SA WG3.

10. The AIOTF sends an AIoT Registration Accept message back to the device via the RAN Reader. The message contains the assigned AIoT Device Temporary ID for the AIoT Device.

The AIoT Device receives the AIoT Registration Accept message and uses the AIoT Device Temporary ID for subsequent communication.

11. The AIoT Device sends the event-driven or periodic AIoT Data Transfer Request message including the assigned AIoT Device Temporary ID.

The AIOTF validates the request using the AIoT Device Profile and sends the message to the target AF found in the AIoT Device context directly or via NEF. The AIOTF sends the AIoT Data Transfer Response message to the AIoT Device via the RAN Reader including a new AIoT Device Temporary ID.

#### 6.9.2.2 DO-A procedure for Topology 2



Figure 6.9.2.2-1: Device initiated Registration and Data Transfer procedure for Topology 2

1. During the registration, the UE indicates the support for the UE Reader Capability to the AMF. The AMF checks if the UE is authorized to act as a Reader based on subscription data. The AMF stores the mapping information between candidate UE Reader(s) and the NG-RAN in the local context.

2. The AF requests for the AIoT DO-A activation which may include the External Target Area information and/or information about the target AIoT Device(s) together with an indication for the use of the UE Reader to the NEF.

Editor’s note: How to coordinate and handle requests from multiple AFs is FFS.

3. The NEF selects the AIOTF(s) as described in clause 5.3.1 of TS 23.369 [3] and sends the AIoT DO-A activation request from the AF to the selected AIOTF(s).

4. The AIOTF selects the AMF considering the Target Area information if received in Step 2 or based on local configuration.

The AIOTF, based on the indication for the use of the UE Reader in the request or based on local configuration to select UE reader(s), retrieves/subscribes to the AMF to obtain the available UE Reader(s) for the selected NG-RAN and selects UE Reader(s). The AIOTF may also consider the stored last known UE Reader information if available e.g. by means of prior Inventory procedure.

5. The AIOTF sends the AIoT DO-A activation response to the AF via NEF.

6. The AIOTF sends the DO-A activation request to the selected AMF including the Requested Service Area Information and/or the AIoT Identification Information together with the authorized UE reader information (e.g. a list of RAN UE NGAP ID(s)).

Editor’s note: The detailed parameters to be included in the DO-A activation request is FFS.

Editor’s note: How the AIOTF gets the RAN UE NGAP ID(s) is FFS.

The AMF selects serving NG-RAN node corresponds to the UE Reader selected by the AIOTF.

NOTE 1: The aspects of NG-RAN selection and UE Reader selection depends on the outcome of KI#1 study.

7. The NG-RAN provides the authorized UE Reader with the access parameters related to Random Access based on the DO-A activation request from the AIOTF, which the UE Reader then periodically broadcasts access parameters related to Random Access for AIoT Device for autonomous transmissions.

NOTE 2: The mechanism for broadcasting access parameters needs coordination with RAN WGs.

8. The AIoT Device listens to access parameters from the UE Reader and performs Random Access to establish the AS connection with the UE Reader.

9. The AIoT Device transmits the AIoT Registration Request message including the AIoT Device Permanent Identifier to the UE Reader. The UE Reader receives the request and forwards the AIoT Registration Request to the NG-RAN and the NG-RAN, aware of which AIOTF the message from UE Reader is destined by step 6, sends the received request to the AIOTF via an AMF.

Editor’s note: Whether and how the privacy protection for the AIoT Device Permanent Identifier applies is FFS.

10. The AIOTF validates the AIoT Registration Request message with DO-A capability of the AIoT Device and the target AF information in the AIoT Device Profile Data provisioned, the Target Area information and/or information about the target AIoT Device(s) configured or received in Step 2.

If validation fails, the AIOTF issues failure response to the AIoT Device and the rest of the procedure is not performed.

Upon successful, the AIOTF updates the AIoT Device Profile Data in the ADM with the Last known AIOTF information.

The AIOTF retrieves the AIoT Device Temporary ID from the ADM, associating it with the last known UE Reader and the target AF and stores the mapping between the UE Reader ID, AIoT Device Temporary ID and the AF ID in the AIoT Device context.

NOTE 3: The security aspects for authentication, authorization and the use of AIoT Device Temporary ID needs coordination with SA WG3.

11. The AIOTF sends an AIoT Registration Accept message back to the AIoT Device via the AMF, NG-RAN and the UE Reader. The message contains the assigned AIoT Device Temporary ID for the AIoT Device.

The AIoT Device receives the AIoT Registration Accept message and uses the AIoT Device Temporary ID for subsequent communication.

12. The AIoT Device sends the event-driven or periodic AIoT Data Transfer Request message including the assigned AIoT Device Temporary ID.

The AIOTF validates the request using the AIoT Device Profile and sends the message to the target AF found in the AIoT Device context directly or via NEF. The AIOTF sends the AIoT Data Transfer Response message to the AIoT Device via the UE Reader including a new AIoT Device Temporary ID.

### 6.9.3 Impacts on services, entities and interfaces

AIoT Device:

- Support to initiate the registration request message based on the access parameters broadcasted by the Reader.

- Support to receive the temporary ID to be used for subsequent autonomous message.

Reader (RAN / UE Reader):

- Support to broadcast access parameters for the DO-A capable AIoT Device(s).

- Support to receives AIoT Device initiated registration and data transfer messages and forwarding it to the AIOTF.

AIOTF:

- Support procedures for handling the AF request for the DO-A activation and DO-A capable AIoT Device initiated registration and data transfer.

- Support to validate requests from DO-A capable AIoT Device, context creation, authentication and authorization, temporary ID assignment.

- Support to route the message between the DO-A capable AIoT Device and the AF.

## 6.10 Solution #10: DO-A Data Delivery and Routing

### 6.10.0 High-level Solution Principles

The solution is based on the following general principles to support DO-A delivery from DO-A capable AIoT devices:

- The target address(es) of the AIoT device are stored in the AIoT Device Profile data, which are provided in the subscribe request from the AF.

- The DO-A capable AIoT devices sends DO-A data over AIoT NAS between the AIoT devices and the AIOTF.

- The AIOTF forwards the DO-A data to the target AF address(es) obtained from AIoT Device Profile data.

### 6.10.1 Description

This solution addresses KI#2 and focuses on the following aspects:

- How an AIoT Device sends data to the AIOTF autonomously.

- Support for routing the data received by AIOTF from an AIoT Device to an AF.

This solution assumes the AIoT device has registered towards the network (i.e., the AIOTF), and have the security contexts established between between the AIoT devices and the AIOTF.

The AIOTF updates its supported domain information or AIoT Device Permanent ID ranges in the NF Profile to the NRF. The NRF supports the AIOTF discovery based on target device information.

The AF subscribes to the DO-A Data Delivery by sending a Subscribe Request to the AIOTF (optioally via the NEF). After receiving the Subscribe Request to the DO-A Data Delivery, the AIOTF performs AF authorization by checking the AF authorization data. If the AF request is authorized, the AIOTF updates the target address(es) provided in the Subscribe Request into the AIoT Device Profile Data in ADM.

The DO-A capable AIoT devices sends DO-A data over AIoT NAS between the AIoT devices and the AIOTF. For example, the AIoT Device sends NAS DO-A Delivery Request to the AIOTF containing the AIoT Device ID and DO-A data. The AIOTF acknowledges the AIoT Device by sending NAS DO-A Delivery Response. The NAS DO-A Delivery Requeust and DO-A Delivery Response are security protected.

NOTE: The form of AIoT Device ID and the security protection of the NAS DO-A Delivery Request/Response are to be addressed by SA3.

The AIOTF obtains the target address(es) from the AIoT Device Profile Data in ADM, and forwards the DO-A data to the target address(es) together with the AIoT Device Permanent ID.

### 6.10.2 Procedures

#### 6.10.2.1 Subscribe to DO-A Data Delivery



Figure 6.10.2.1-1 Subscribe to DO-A Data Delivery

Figure 6.10.2.1-1 depicts how the AF subscribes to the DO-A data delivery:

1. The AF sends Subscribe Request to the NEF for DO-A data delivery with the AF ID, target device information (AIoT Device Permanent IDs or Filtering Information) and target address (i.e., notification endpoint of the AF). For AFs in trusted domain, the AF can send Subscribe Request to the AIOTF directly without involving the NEF.

2. The NEF discovers the AIOTF by providing target device information to the NRF or based on local configuration. The NEF sends the Subscribe Request to the AIOTF for DO-A data delivery with the AF ID, target device information and target address (i.e., notification endpoint of the NEF).

3. The AIOTF authorizes the AF request to check whether the AF is allowed to subscribe to DO-A delivery, based on the AF authorization data stored in the ADM.

4. If authorized, the AIOTF updates AIoT Device Profile data with the target address for the target devices. If the target device information from the AF is Filtering Information, the AIOTF needs to update the AIoT device profile data for each device in the group. Alternatively, the AIOTF may send the Filtering Information to the ADM and the ADM is responsible for the updating for each device in the group.

The target address is the notification endpoint of the NEF or the notification endpoint of the AF, depends on which NF sends the Subscribe Request.

5. The AIOTF sends Subscribe Response towards the NEF indicating the result of the subscribe. In case of failure, failure cause is included. In case of succeed, subscription correlation ID is included.

6. The NEF sends Subscribe Response to the AF indicating the result of the subscribe. In case of failure, failure cause is included. In case of succeed, subscription correlation ID is included.

#### 6.10.2.2 DO-A Data Delivery



Figure 6.10.2.2-1 DO-A Data Delivery

Figure 6.10.2.2-1 depicts how DO-A data are delivered from the AIoT device towards the AF:

1. The AIoT Device sends AIoT NAS DO-A Delivery Request to the AIOTF with the Device ID and DO-A data.

For topology 1, the AIoT NAS message is delivered via the RAN reader inside NG-RAN node. The NG-RAN node delivers the NAS message to the AIOTF directly or via the AMF.

For topology 2, the AIoT NAS message is delivered via the UE reader. The UE reader delivers the message to the NG-RAN node, and the NG-RAN node delivers the NAS message to the AIOTF via the AMF.

NOTE 1: The details of AIoT Device ID and the security protection of the NAS DO-A Delivery Request/Response are to be addressed by SA3.

NOTE 2: The NG-RAN and the AMF are assumed to route the AIoT NAS DO-A Delivery Request to the AIOTF which holds the AIoT device contexts in the Registration Procedure.

Editor’s Note: If the request is routed to a new AIOTF, how the new AIOTF fetches the AIoT device contexts from the old AIOTF is FFS.

1. The AIOTF authenticates the AIoT device and sends the NAS DO-A Delivery Response to the AIoT Device. The result is included in the response message. In case of failure, the failure cause is included.

NOTE 3: The authentication is to be addressed by SA3.

3. The AIOTF gets the target address(es) of the AIoT device from the AIoT Device Profile data. For each target address, step 4 to step 7 are executed individually.

4. The AIOTF sends Notify message to the NEF with the AIoT Device Permanent ID and DO-A data, if the target address is the notification endpoint of the NEF. If the target address is the notification endpoint of the AF, the AIOTF sends Notify Request to the AF directly without involving the NEF.

5. The NEF sends Notify message to the AF with the AIoT Device Permanent ID and DO-A data.

### 6.10.3 Impacts on Services, Entities and Interfaces

The following NFs are impacted::

- AIOTF:

- AIoT NAS layer support for DO-A Data Delivery.

- Notify DO-A data to the target address(es) obtained from AIoT Device Profile Data in ADM.

- Support subscribe request towards the DO-A data delivery.

- Perform AF authorization for the subscribe request. If authorized, the AIOTF update the AIoT Device Profile data to include the target address provided in the subscribe request.

- ADM:

- Enhance AF authorization data for the subscribe request towards DO-A data delivery.

- Enhance AIoT Device Profile data for the target address(es).

- NEF:

- Support subscribe request towards the DO-A data delivery.

- Notify DO-A data to the AF.

- NRF:

- Support domain information or AIoT Device Permanent ID ranges in the NF Profile of the AIOTF.

- Support AIOTF discovery based on target device information.

- AIoT Device:

- AIoT NAS layer support for DO-A Data Delivery.

## 6.11 Solution #11: DO-A device registration and uplink data transmission

### 6.11.0 High-level Solution Principles

The solution is based on the following general principles:

- The DO-A capable AIoT Device performs the active registration procedure towards the AIOTF.

- The NG-RAN selects the AIOTF based on the stored AIOTF information, or AIOTF information contained in the AIoT Device ID, or local configuration.

- ADM is enhanced with the allowed/subscribed AF information, which is used by the AIOTF to determine the target AF for the uplink data transmission from DO-A capable device.

- AIOTF can retrieve the AIoT Device context from the last serving AIOTF that further includes the service-related information.

It addresses the KI#2.

### 6.11.1 Description

This solution mainly focuses on the DO-A capable device and includes two crucial parts: device-initiated registration procedure and the uplink DO-A data transmission from the Device to the AF. Some of the key procedures are listed below:

1) DO-A capable AIoT Device actively sends the device registration request to the network, that includes the Device ID, security parameters, registration type.

- Registration type: Similar to UE, AIoT Device can indicate to the network about its registration type, e.g., periodic registration, initial registration, mobility registration. Alternatively, the AIOTF or the NG-RAN/RAN reader can determine the registration type for the AIoT device based on the locally stored device context.

2) The AIOTF selection at the NG-RAN can be based on different options:

- NG-RAN selects the AIOTF based on OAM local configuration.

- NG-RAN selects the AIOTF based on locally stored AIOTF information, e.g., from the past procedures as device context.

- NG-RAN selects the AIOTF based on the Device ID, e.g., AIOTF ID included in the temporary Device ID.

3) The Routing from AIOTF to the AF can be based on two different options:

- AIOTF checks the information in the ADM that further includes the subscribed/allowed AF information (e.g., AF ID).

- AIoT Device sends the AF ID to the AIOTF.

4) Context management of the AIoT Device among AIOTF and ADM：

- AIOTF stores the device registration information that contains registration area and registration status, and may also store it at ADM.

- AIOTF retrieves the device context from the last serving AIOTF, that including the security parameters, device last serving reader, and service-related information (a.k.a., service context). The service context includes the requested AF ID, transaction ID, target area information, and other service specific information, e.g., assistance information for inventory and command. The service context can be used by the AIOTF to autonomously initiate the service towards the AIoT Device if it just moves within its serving area, without further receiving the service request from the AF.

### 6.11.2 Procedures



Figure 6.11.2-1 DO-A Device registration and Uplink data transmission

0: AIoT Device obtains radio resource for D2R message.

Editor's note: How AIoT Device obtains radio resource for D2R message is FFS and is to be decided by RAN WGs.

1: AIoT Device sends a D2R message to NG-RAN with device registration request, that includes the Device ID, registration type (e.g., periodic registration, mobility registration, initial registration), and security parameters.

Editor’s Note: The details of the AIoT Device ID that is used in the registration request is FFS.

The trigger for the AIoT Device performing registration towards the network can be e.g., when device has data pending to report, or when periodic registration is needed (either triggered by device or by the Reader or AIOTF performing periodic inventory), or when mobility registration condition is met (e.g., based on the registration area).

Editor's note: The details for triggering the mobility registration of AIoT Device is FFS.

2: NG-RAN selects the AIOTF based on local configuration by OAM, or by checking the AIOTF information contained in the Device ID (e.g., temporary ID), or based on the locally stored AIOTF information from the past procedures associated with the AIoT Device, e.g., device context that contains the serving AIOTF information.

Editor’s Note: Whether the NG-RAN has the device context that contains the AIOTF information is FFS.

NOTE: The temporary ID design needs to be addressed by the SA3.

3: NG-RAN sends the registration request to the selected AIOTF, either directly, or via the AMF. If via the AMF, the AIOTF ID is also included.

4: Optionally, The AIOTF can retrieve the device context from the last serving AIOTF based on the last serving AIOTF information contained in the Temporary Device ID, or received from ADM. The retrieved device context can contain the security parameters, last serving reader information of the Device, service-related information (a.k.a., service context). The service context can include the AF ID (that sent the service request for the device before device moves to the serving area of the current AIOTF), transaction ID, target area information and other service specific information, e.g., assistance information for inventory and command.

5: AIOTF performs the verification of the AIoT Devices, checks whether the data transmission from the device is allowed, and stores/updates the device profile information in the ADM, e.g., updating the serving AIOTF information for the AIoT Device. The AIOTF will store the device registration information either locally, or at the ADM, that includes the registration status (registered), and the device registration area.

Editor’s Note: Details of authentication procedures will be determined by SA3.

6: The ADM informs the old/last serving AIOTF (AIOTF2 in the Figure) with device ID that it is no longer the serving AIOTF for the AIoT Device and the device context can be released if any.

7: AIOTF sends the device registration response message to the NG-RAN and AIoT Device, either directly, or indirectly (via AMF). It contains the Device ID (can be a new temporary ID), registration accept/reject (with a cause and skip all the following messages), registration area for the device.

8: After receiving the registration response (that may include the data transmission accept indication), AIoT Device sends the DO-A message to the NG-RAN/RAN reader, that includes the Device ID, DO-A data, expected D2R message size (sent to RAN reader /NG-RAN for assistance of radio resource allocation), AF ID (optional), where the DO-A data is encrypted in the AIOT NAS message between the AIoT Device and AIOTF.

NOTE: The expected D2R message is sent from AIoT Device to the NG-RAN/RAN reader and can happen before the transmission of actual DO-A data, and depends on RAN2 discussion.

Editor’s Note: Whether the AF ID can be provided by the AIoT Device to the network is FFS.

9: After selecting the AIOTF (as described in Step 2), NG-RAN sends the DO-A message that contains the Device ID, reader ID, DO-A data, , target AF information (optional) and AIOTF ID (if AMF in between).

10: If no AF ID is explicitly sent by the AIoT Device, AIOTF can check the subscribed/allowed AF information from the ADM using Device ID as the key. It is assumed that the ADM is enhanced with the allowed/subscribed AF information, meaning it can receive the data from the DO-A capable device. The allowed/subscribed AF information is pre-configured in the ADM based on the SLA between the MNO and the 3rd party AF.

11: AIOTF sends the DO-A data, Device ID and AF information to the NEF.

Editor’s Note: The determination of NEF for routing the DO-A data from AIOTF to the AF is FFS.

12: The NEF forwards the AIoT Device ID, DO-A Data to the AF based on the AF information sent by the AIOTF.

### 6.11.3 Impacts on Services, Entities and Interfaces

**AIOTF:**

- Determine the target AF for sending the DO-A data from AIoT Device to the AF

- Support registration management of the AIoT Device

- Interaction with last serving AIOTF for Device context retrieval

**NG-RAN:**

- Determine the target AIOTF to forward the uplink message from AIoT Device

**ADM:**

- Store the subscribed/allowed AF information for the AIoT Device data report

**AIoT Device:**

- Performs the active registration procedure towards the network

- Sends the DO-A data to the AF via the network

## 6.12 Solution #12: Enable DO-A traffic with MICO like mechanism

6.12.1 Description

#### 6.12.1.1 High-level solution principles

This solution applies to topology 1.

AIoT device can support inventory and command. In order to help the DO-A capable AIoT device with limited energy storage capability to save power, a DOO (device originated only) mode and DOO mode related Active Time is used.

The AF may request the network to configure a DO-A capable AIoT device to use the DOO mode and DOO mode related Active Time using enhanced command procedure with a new Command Type: Configure.

During the enhanced command procedure, the device could be configured to use the DOO mode and a DOO mode related Active Time value that is used to indicate the duration during which the device can send uplink AIoT traffic and receive the downlink AIoT traffic. During the enhanced command procedure the AIoTF ID and the AF routing information are sent from the AIoTF to the device to route the DO-A NAS message and DO-A data.

A timer corresponding to the DOO mode related Active Time value is started or restarted by the AIoT device when the uplink AIoT traffic is sent out from the device. After the timer expires the DOO mode is activated in the device. The DOO mode is deactivated when there is DO-A data to be sent out from the device. A counterpart timer is used in AIoTF.

NOTE: The AIoT devices configured with DOO mode are assumed not applicable for Inventory service from AF perspective.

Editor’s note: Timer for the DOO mode related Active Time duration in this solution is FFS.

#### 6.12.1.2 Definition

**AF routing information**: used to select NEF, for example AF ID, FQDN or IP address of the AF.

**DO-A data**: AIoT data related to the DO-A traffic.

**DO-A NAS message**: an AIOT NAS message that is sent from the AIoT device and includes the AIoT device ID and DO-A data.

**DOO (Device Originated Only) mode:** An AIoT device that has activated the DOO mode does not need to receive downlink AIoT traffic.

**DOO mode related Active Time:** An AIoT device that is in DOO mode related Active Time duration is able to receive downlink AIoT traffic and send uplink AIoT traffic.

NOTE: The feasibility of using timer in AIoT device depends on the RAN WG.

**downlink AIoT traffic**: includes paging message related to the inventory procedure, and NAS Command Request message.

**uplink AIoT traffic**: includes AIOT NAS message that responds to the paging message related to the inventory procedure, NAS Command Response message, and DO-A NAS message.

6.12.2 Procedures

#### 6.12.2.1 enhanced command procedure to configure AIoT device



Figure 6.12.2.1: enhanced command procedure to configure AIoT device

0. The AIoT device supports inventory and command procedure.

1. The AF sends the Nnef\_AIoT\_Command message to NEF as specified in the step 1 of clause 6.2.3 TS 23.369 with the following additional clarification:

The Nnef\_AIoT\_Command message additionally includes: a DO-A service indicator, a DOO mode indication, and a DOO mode related Active time value. The DO-A service indicator is used to indicate that the AIoT device related with the device ID can initiate DO-A service. The DOO mode indication indicates the AF's preference for DOO mode for the AIoT device. The DOO mode related Active time value indicates how long the DOO mode related Active Time duration is.

The Command Type is set to Configure to request to negotiate and configure the DOO information (i.e. the DOO mode and the DOO mode related Active time value) for the AIoT device.

The NEF selects the AIOTF(s) as described in TS 23.369 [3].

The AIOTF authorize the AF, selects the AIoT reader(s), and response to the AF as described in TS 23.369 [3].

The AIOTF store the DO-A service indicator in the ADM, determine and store the DOO mode indication, the DOO mode related Active time value in the AIoT device profile related with device ID in the ADM based on the request from the AF, local configuration, and the policy of the network.

2. Step 7 of Command procedure specified in clause 6.2.3 in TS 23.369 [3].

3. Step 8 of clause 6.2.3 Command Procedure in TS 23.369 [3] with the following additional clarification:

If the inventory reports include the device ID that corresponds to the device ID received by the AIOTF in step 1, the AIOTF sends Command Request message to the corresponding reader and the Command Request message additionally includes a DO-A service indication that is used to assist NG-RAN to provide DO-A service network resource information to the AIoT device;

The NAS Command Request includes a DOO mode indication, a DOO mode related Active time value, the AF routing information, and the AIOTF ID.

4. Step 9 of clause 6.2.3 Command Procedure in TS 23.369 [3] with the following additional clarification：

If the DO-A service indication is received in step 3, the AIoT Reader provides DO-A network resource information to the device in the AS R2D message.

5. After receiving the AS R2D message and the NAS Command Request in step 4:

The device stores DOO mode indication, the DOO mode related Active time value, the AIOTF ID, and the AF routing information, and the DO-A network resource information; and

The AIoT device shall set a timer corresponding to the DOO mode related Active Time value received.

6. Step 10 of clause 6.2.3 Command Procedure in TS 23.369 [3] with the following clarification:

After the NAS Command Response is sent out, the AIoT device shall start the timer corresponding to the DOO mode related Active Time value if the DOO mode related Active Time value is not zero and the device stores DOO mode indication. If the Time value is zero and the device stores DOO mode indication the AIoT device activate DOO mode immediately.

When the timer expires (i.e. reaches the DOO mode related Active Time value) the AIoT device activates DOO mode and is not available for receiving downlink AIoT traffic.

7. Step 11~13 of Command procedure in clause 6.2.3 in TS 23.369 [3] with the following clarification:

After the NAS Command Response is received, the AIOTF shall start the timer corresponding to the DOO mode related Active Time value if the DOO mode related Active Time value is not zero and the device is indicated the DOO mode indication. If the Time value is zero and the device stores DOO mode indication the AIOTF can deduce that AIoT device has activated DOO mode. When the timer expires the AIOTF can deduce that the AIoT device has activated DOO mode and is not available for receiving downlink AIoT traffic.

Editor’s note: The impact of the DOO mode to the AS layer in AIoT device is FFS.

#### 6.12.2.2 DO-A procedure



Figure 6.12.2.2-1: DO-A Procedure

0. The AIoT device capable of DO-A is configured with DOO mode indication, stores a DOO mode related Active time value, AIOTF ID, and AF routing information, and the DO-A network resource information using the device configuration procedure. It is assumed that the AIoT device has activated DOO mode.

1. When there is DO-A data needed to be sent to the network, the AIoT device deactivate the DOO mode and sends AS D2R message (AIOTF ID, DO-A NAS message) to the NG-RAN based on the stored DO-A network resource information. The AIOTF ID is used by NG-RAN to select AIOTF. DO-A NAS message includes AF routing information, device ID, and DO-A data.

After the DO-A NAS message is sent out:

- if the device stores DOO mode indication and if the stored DOO mode related Active Time value is not zero, the AIoT device shall start the timer corresponding to the DOO mode related Active Time value;

- if the device stores DOO mode indication and if the stored Time value is zero, the AIoT device shall activate the DOO mode immediately.

2. NG-RAN selects the AIOTF based on the AIOTF ID received in step 1.

3. NG-RAN forward the DO-A NAS message to the selected AIOTF together with the reader ID and RAN AIoT Device NGAP ID.

4. The AIOTF authenticates the device corresponding to the device ID carried in the DO-A NAS message.

If the device is authenticated successfully:

- The AIOTF shall start the timer corresponding to the DOO mode related Active Time value if the DOO mode related Active Time value is not zero and the device is indicated to use DOO mode; and

- The AIOTF selects the NEF based on the AF routing information carried in the DO-A NAS message.

If the device failed the authentication, the DO-A NAS message is discarded by the AIoTF.

5. The AIOTF send the DO-A data, the device ID, and AF routing information received in step 3 to the NEF. And NEF forward the DO-A data and device ID to the AF based on the AF routing information.

6. After receiving the DO-A data the AF may subsequently request AIoT service (e.g. Nnef\_AIoT\_Inventory, Nnef\_AIoT\_Command) for the corresponding device. The AIoT service request is sent to the AIOTF.

7. If the device ID related timer corresponding to the DOO mode related Active Time value is running, the AIOTF determines the device could receive the DL AIoT traffic and proceed with the AIoT service. If the device ID related timer expires or is not running and the device has been indicated to use the DOO mode, the AIOTF considers the device has activated the DOO mode and is not able to receive downlink AIoT traffic and may reject the AIoT service, and then the step 8~9 is skipped.

8. The DL AIoT traffic is transferred to the device as described in the inventory and command procedure.

9. When the timer expires (i.e. reaches the DOO mode related Active Time value) the AIoT device activates DOO mode.

6.12.3 Impacts on Services, Entities and Interfaces

AIoT Device:

- support device configuration procedure;

- supports DO-A procedure;

- supports timer;

NG-RAN(including AIoT Reader):

- support device configuration procedure;

- supports DO-A procedure;

AIOTF:

- support device configuration procedure;

- supports DO-A procedure;

ADM:

- support AIoT Device profile including: DO-A service indicator, DOO mode indication, the DOO mode related Active time value

Editor’s note: Other impacts (e.g. impacts on NEF, etc.) is FFS.

## 6.13 Solution #13: Network Triggered Initial Registration

### 6.13.0 High-level solution principles

The key technical principles proposed in this solution are summarized below:

- Network triggers the AIoT Device to perform initial Register using Inventory procedure to trigger un-registered devices to register.

NOTE: Registration due to mobility or periodic registration is assumed to be autonomously done (using the DO-A procedure) by the AIoT Device after the AIoT Device has performed initial registration.

- Reuse of Rel-19 Inventory and Command procedure to support registration of an AIoT Device as specified in TS 23.369 [3]. A Registration Indicator is included in the Inventory Request and paging message.

- Reuse of Rel-19 security solution for authentication and command protection as specified in TS 33.369 [11].

### 6.13.1 Description

This solution proposes to reuse the Inventory procedure and command procedure to support Device registration to the network. This allows re-use of rel-19 security procedures i.e., authentication, privacy protection and command protection.

Key Procedures:

- AF invokes a new network service to register AIoT Device(s). The AF may include e.g. External Target Area information to aid the network to select AIOTF and where perform Inventory to trigger initial registration for specific AIoT Devices.

- The AIOTF can trigger the initial registration without an AF service invocation. In this case the AIOTF determines the periodicity and selection of NG-RAN(s) based on AIOTF implementation. The AIOTF will not include the AIoT Identification Information in the Inventory Request message to trigger all AIoT Devices that are not registered.to respond.

- A Registration indication is included in the Inventory Request to restrict the responses to only from AIoT Devices that are not registered to the network.

- The AIOTF uses the Inventory procedure to trigger the AIoT Device to check if it is registered to the network. The PLMN ID or NID must be provided in the paging message (see the procedure below for more details).

- Un-registered AIoT Device(s) includes an indication to register in the Inventory Response message. As specified in rel-19 the Inventory Response message includes protected information that the network uses to derive the AIoT Device Permanent Identifier and to authenticate the AIoT Device.

- The AIOTF sends a Command (based on rel-19 functionality) with a Registration Accept message. This message includes the necessary information for the device to enable DO-A transmission. The details of the parameters and information will be identified in solutions for the DO-A transmission and security aspects specified by SA3 for DO-A transmissions.

### 6.13.2 Procedure



Figure 6.13.2-1: Procedure for network triggered registration.

0. The AIoT device profile per AIoT Device is provisioned in the ADM.

1. The AF invokes Nnef\_AIoT\_Registration Request in service operation request to the NEF. The Request includes same parameters as Nnef\_Inventory Request as specified in TS 23.369 [3].

2. The NEF may further authorize the AF request, selects AIOTF and invokes the Naiotf\_AIoT\_Registration service operation towards each of the selected AIOTF(s). The Request includes same parameters as Naiotf\_Inventory Request as specified in TS 23.369 [3].

3. The AIOTF receives the Naiotf\_AIoT\_Registration request and checks the parameters included in the request. The AIOTF may perform authorization of the AF as specified in clause 5.6 in TS 23.369 [3]. The AIOTF prepares the Inventory Request to be sent to the NG-RAN. The AIoT Identification Information to be included in the paging message includes the PLMN ID or NID i.e., the Filtering Information includes the PLMN ID or NID part.

Editor's note: It is FFS whether and how to provide PLMN ID or NID when single AIoT Device is paged with a Temporary ID.

4. AIOTF sends the AIoT Registration Service Response to the NEF containing the accept or reject result for the AIoT service operation request based on step 3.

5. NEF sends the AIoT service operation response to the AF, containing the accept or reject result for the AIoT service operation request as specified in clause 8.3 in TS 23.369 [3].

6. Same as step 7 in the Inventory procedure specified in TS 23.369 [3] with the additional Registration Indicator included in the Inventory Request. If triggered by an AF the Inventory Request includes the AIoT Identification Information corresponding to the AF request.

This step can be performed by the AIOTF without receiving the service request from an AF, in this case the AIOTF determine the periodicity and selection of NG-RAN(s) based on AIOTF implementation. If AIOTF triggers the initial registration, then the Inventory Request will not include the AIoT Identification Information to trigger all AIoT Devices that are not registered.

7. Same as step 9 in the Inventory procedure specified in TS 23.369 [3] with the additional Registration Indicator included in the paging message.

8. The AIoT Device determines whether it matches the AIoT Identification Information as specified in step 9 of the Inventory procedure specified in TS 23.369 [3].

The AIoT Device checks the PLMN ID or NID and whether the AIoT Device is registered or not. In case the AIoT Device is not registered, the AIoT Device includes a Registration Request Indication in the AIOT NAS message. The AIOT NAS message also includes the parameters as specified in step 9 of the Inventory procedure specified in TS 23.369 [3].

9. Same as step 10 in the Inventory procedure specified in TS 23.369 [3].

10. Same as step 11 in the Inventory procedure specified in TS 23.369 [3].

11. For each successful Registration Request received, the AIOTF prepares a NAS Registration Accept message and includes the NAS Registration Accept message in the Command Request message. The rest of this step is as specified in step 8 in Command procedure specified in TS 23.369 [3].

NOTE 1: Detailed list of parameters to be included in the NAS Registration Accept message will be determined in coordination with SA3 to support DO-A message transmissions.

12. Same as specified in step 9 in Command procedure specified in TS 23.369 [3].

13. Same as specified in step 10 in Command procedure specified in TS 23.369 [3]. The Command Response includes the NAS Registration Complete message.

14. Same as specified in step 11 in Command procedure specified in TS 23.369 [3]. The Command Response includes the NAS Registration Complete message.

15. The AIOTF updates the AIoT Device Context and the AIoT device profile in the ADM that the AIoT device is registered with the network.

16. The AIOTF reports the result of the Naiotf\_AIoT\_Registration request to the NEF by sending the Naiotf\_AIoT\_Registration Notify message (a list of AIoT Device(s) response information (AIoT Device ID(s), Registration status and optionally location of each AIoT Device), AF ID, [Last Report Indication]). If multiple AIOTFs are involved in the procedure, the NEF may receive Naiotf\_AIoT\_Registration Notify messages from multiple AIOTFs.

NOTE 2: The above parameters are the same as included in the Naiotf\_AIoT\_Inventory Notify message.

NOTE 3: In case multiple AFs are included in the AIoT Device Profile, then all AFs will be notified about the initial registration event.

17. The NEF informs the AF of the result of the Nnef\_AIoT\_Registration request by sending the Nnef\_AIoT\_Registration Notify message (a list of AIoT Device(s) response information (AIoT Device ID(s), Registration status and optionally location of each AIoT Device), AF ID, [Last Report Indication]).

### 6.13.3 Impacts on Services, Entities and Interfaces

NEF:

- Support new Nnef\_AIoT\_Registration service.

AIoT Device:

- Support Registration procedure including:

1. Verify whether it is registered in the specific network,

2. Receive Registration Accept message and

3. Use the parameters included in the accept message and respond with a Register Complete message.

AIOTF:

- Support Registration service procedure:

1. Invocation of the service by the NEF/AF

2. Receiving in the NAS Inventory Response and indication that the AIoT Device requests to register in the network.

3. Configure the AIoT Device with parameters included in the Registration Accept message.

ADM:

- Maintain the AIoT Device Profiles with registration status information.

NG-RAN:

- None

AIoT Reader:

- None

## 6.14 Solution #14: DO-A capable AIoT Device Registration Procedure

### 6.14.0 High-level solution Principles

DO-A capable AIoT devices possess the capability to transmit MO signalling and data. Furthermore, the AIoT device actively registers with the core network to notify it of its presence autonomously.

### 6.14.1 Description

This solution addresses KI#2, specifically concerning the method by which the DO-A capable AIoT device can autonomously notify the network of its presence for Topology 1.

In this solution, it is assumed:

- The AIoT device actively initiates the registration process with the network. The registration types include:

A. initial registration.

B. mobility registration update.

C. Periodic registration.

- ADM stores the DO-A capable AIoT device profile information.

- AIOTF handles NAS termination and device authentication for DO-A capable AIoT devices and manages registration and mobility for AIoT Devices.

### 6.14.2 Procedures

11. ADM stores the serving AIOTF

12. ADM initiates context release procedure with the old serving AIOTF

8. AIoT device replies with registration complete

9. AMF forwards the registration complete to AIOTF

10. AIOTF notifies the ADM of registration status

7. AIOTF responses the Registration accept to the AIoT Device

6. AIoT Device Authentication and Authorization

4. gNB forwards the registration to the serving AIOTF

5. AIOTF fetches context information from the previous serving AIOTF

0.AIoT Device profile provisioning in ADM

2. AIoT Device initiates registration procedure

1.AIoT Device meets the trigger conditions

AIoT Device （DO-A）

AMF

ADM

New AIOTF

gNB

Old AIOTF

3.gNB discovers the serving AIOTF

Figure 6.14.2.1: DO-A capable AIoT Device Registration Procedure

0. The DO-A capable AIoT Device’s subscription data is provisioned in the ADM

Editor’s Note: The subscription data of a DO-A capable AIoT device is FFS.

1. The DO-A capable AIoT Device meets the following trigger conditions, then it will send a NAS Registration Request to the core network.

The AIoT Device performs an Initial Registration if it is not registered with the network.

The AIoT Device performs Mobility Registration if it has moved outside of its AIoT Registration Area.

The AIoT Device performs periodic registration if it has registered on the network and remains in its AIoT Registration Area beyond the designated time period.

Editor’s Note: The details of the AIoT Registration Area need to align with the RAN WG

2. AIoT Device sends a message to NG-RAN, including a NAS Registration Request (Registration Type, Temporary ID, device information, security parameters). Registration can be initial registration, mobility registration, or periodic registration. Then, NG-RAN sends the Registration Request to the selected AMF.

3. The gNB discovers the serving AIOTF.

Editor’s Note: The details of how the gNB discover the serving AIOTF are FFS.

4. The gNB forwards the registration request to the serving AIOTF by either direct connection or indirect connection via the AMF.

5. [Conditional] The serving AIOTF determines the old AIOTF using the temporary ID and retrieves the AIoT Device context from the old AIOTF.

6. The AIOTF performs the Authentication/Security procedure and stores the security context.

Editor’s Note: Details of authentication/security procedures will be determined by the SA3 WG.

7. The AIOTF responds the Registration Accept to the AIoT device , including a new temporary ID assigned by the serving AIOTF, AIOT Registration Area, and periodical registration timer.

8. The AIoT device responds to the AIOTF with Registration Complete via NG RAN and AMF.

9. The AMF forwards the Registration complete to the AIOTF.

10. The AIOTF notifies the ADM of the registration complete status about the AIoT device.

11. The ADM stores the serving AIOTF for the AIoT device.

12. [Conditional] If the ADM discovers that the serving AIOTF has changed, then it needs to initiate the context release procedure to the old AIOTF to delete the context in it.

### 6.14.3 Impacts on Services, Entities and Interfaces

**AIOTF:**

- Support Registration and Mobility Management.

**NG-RAN:**

- Supports the AIOTF selection and transferring NAS messages to and from the AIoT Device.

**AIoT Device:**

- Support performing the registration procedure.

**ADM:**

- Support new interface with AIOTF.

## 6.15 Solution #15: Support reliable time-base Data Collection of DO-A AIoT sensor device with network trigger

### 6.15.0 High-level solution Principles

This solution addresses KI #2 to support DO-A sensor data collection with network assistance, with the following key principles:

1. The AF starts the time-based (e.g. periodic or at certain time) data collection service from the DO-A sensor device(s) by sending the AIoT command request to NEF, with the assumption that all the DO-A sensor device(s) for this operation have been registered with the 5G network before the service starts( e.g. DO-A sensor device can autonomously register to the network without the trigger from network)

NOTE 1: How the DO-A sensor device registers to the network is not covered in this solution and other DO-A device registration solutions can be applied.

2. The data collection pattern of the AIoT sensor device(s) (e.g. periodic and aperiodic time-based data collection) is configured and aware by the AF. The AF provides the data collection pattern information to the AIoTF, which also provides the information to the NG-RAN / AIoT reader(s) to coordinate the data collection.

3. The AIoTF provides the assistance information to the AIoT reader(s) or the NG-RAN to assist time-based (e.g. periodic or aperiodic) data collection (e.g. pre-allocate resource and send triggers for the DO-A sensor device(s)). The assistance information includes periodic data collection information (e.g. start or end time of data collection, interval between periodic data collection, or certain point of time when the data collection is needed, so on).

4. For periodic data collection, the AF and the AIoTF use single command procedure as defined in TS 23.369 to start the time-based data collection operation from DO-A AIoT device(s), without sending read command for every periodical data collection cycle. The AIoT reader periodically trigger and allocated radio resource for the data collection of the AIoT sensor device(s), based on the assistance information from the AIoTF.

5. This solution only focuses on time-based (e.g. periodic or at certain time) data collection of DO-A device(s) and doesn’t prevent DO-A device(s) transmitting data autonomously (e.g. event trigger transmission).

NOTE 2: The trigger and resource allocation mechanisms of AIoT reader are determined by RAN WGs and the coordination with RAN WGs is needed.

NOTE 3: Security consideration for periodic data collection operation will be determined by SA3.

Editor’s note: How to support DO-A device mobility is FFS.

### 6.15.1 Description

One of the key DO-A use cases is time-based (e.g. periodic ) data collection from AIoT sensor. Considering the nature of DO-A IoT device which is still a low energy and low complex device, keeping accuried and network-sychronized clock for periodic data transmission in the AIoT sensor is challenging. Although DO-A device can autonoumously sending data, a large number of AIoT sensor device sending periodic data at the promiximty time without network coordination can cause serious race condition for the network resource which lead to low effective of data collection. This solution allows AIoT reader, with the time-based data collection assistance information provided by AIoTF, to periodically or at-certain point to preallocate radio resouce and trigger the DO-A AIoT sensor device to send sensor data when the transmission time is come. With this solution, the DO-A sensor device doesn’t need to maintain a timer which is need to be synchronized with network or AF for periodic transmission.

### 6.15.2 Procedures



Figure 6.15.2-1 periodic data collection

1. Step 1 to step 6 of Procedure for Command in clause 6.2.3 of TS 23.369 [3] with additional parameters. AF sends AIoT Command Request to NEF. In includes Device(s) Info, Location (External), AF Transaction ID, Command Type Read, Length, Periodic data collection indication, Approximate number of AIoT Devices, and periodic data collection Parameters (periodic data collection start / end time, interval between each data collection cycle). NEF selects AIOTF, and then NEF sends AIoT Command Request to AIOTF. AIOTF checks AF Authorization by retrieving AF Authorization Profile in ADM. AIOTF sends AIoT Command Response to NEF. It includes Status (Success/Failure), Transaction ID. NEF sends AIoT Command Response to AF. It includes Status (Success/Failure), AF Transaction ID.

2. Step 7 to step 10 of Procedure for Inventory in clause 6.2.2 of TS 23.369 [3]

3. AIOTF sends AIoT Command Request to AIoT Reader via NG-RAN. This includes Device ID, (Reader ID), Command Type Read, Correlation ID, Length, and assistance information which includes Periodic data collection indication and periodic data collection Parameters (periodic data collection start / end time, interval between each data collection cycle). AIoT Reader stores Correlation ID with AIoT Device ID as context data as well as the assistance information.

4-5. When the periodic sensor data collection time starts, AIoT Reader sends AIoT Command Request to the AIoT Device. This includes Device ID, (Reader ID), Command Type Read, Correlation ID.

NOTE: AIoT reader or NG-RAN may allocate radio resource for the D2R command response from the DO-A Device. This is up to RAN WG decision.

6. AIoT Device sends AIoT Command Response to AIoT Reader. This includes Device ID, and the data collected from the AIoT device(s).

7. AIoT Reader sends AIoT Command Response to AIOTF. This includes Device ID, Sensing Result, and Correlation ID. AIoT Reader retrieves Correlation ID with AIoT Device ID from the stored context.

8. AIOTF sends AIoT Command Notify to NEF. This includes Device ID, Sensing Result, and Transaction ID. AIOTF retrieves Transaction ID with Correlation ID from the stored context.

9. NEF sends AIoT Command Notify to AF. This includes Device ID, Sensing Result, and AF Transaction ID. NEF retrieves AF Transaction ID with Transaction ID from the stored context.

10-14. Every Period, AIoT reader sends AIoT command Request to the AIoT Device. Repeat step 5-9.

### 6.15.3 Impacts on services, entities and interfaces

Impacts on existing entities:

AIOTF:

- Receives time-based data collection information (e.g. periodic data collection information) from AF

AIoTF:

- Add time-based data collection information to the assistance information, such as

- periodic data collection: periodic data collection indication, interval of each data collection cycle, start or end time of the periodic data collection.

- aperiodic data collection: time(s) when the data collection starts

AIoT Reader:

- Maintain DO-A device context to conduct data collection procedure at certain point of time based on the assistance information.

- Supports periodically start AIoT Command-only read procedure to collect data from AIoT Device(s) with triggering AIoT device(s) to send data.

- For aperiodic data collection, supports triggering AIoT device to send data when the data collection time is up.

## 6.16 Solution #16: AIoT device DOA data detection and collection

### 6.16.0 High-level solution Principles

This solution addresses the DOA traffic enabling aspects of KI#2. The solution proposes the procedures for the AIoT Readers and the network to detect and collect the AIoT device’s DOA data. The solution assumes that the AIoT device broadcasts a signal (“Data Ready Indication”) when it has DOA data to send. The nearby AIoT Readers that detects the signal may then use enhanced R19 Paging and Command procedures to handshake with the device and collect the DOA data from the device.

The solution also describes how the AIoT Reader that has collected DOA data from the device can route the data to the network (i.e. AIOTF) and the AF. The routing of DOA data is based on the AIoT Reader’s local configuration that maps the AIoT identifier information to the AIOTF address.

### 6.16.1 Description

#### 6.16.1.1 Device broadcasted “Data Ready Indication”

When a DOA capable device has data to send, it broadcasts a Data Ready Indication (DRI). The purpose of this broadcast information is to probe whether there is an AIoT Reader that is able to receive its DOA data. The radio resource used for the broadcast may be preconfigured in the device. If the broadcast indication is not immediately picked up by any AIoT Reader and the device doesn’t receive response (e.g. Paging) from AIoT Readers, the device may repeat (e.g., periodically) the broadcast for a preconfigured time duration.

Editor's note: How the AIoT device broadcasts DRI depends on RAN WGs’ design.

An DOA-capable AIoT Reader is preconfigured with the radio resource on which the DRI broadcast may be transmitted and monitors the DRI broadcast from the AIoT devices. If a Reader (e.g., a UE Reader) is not able to monitor this signal all the time, it may monitor the DRI broadcast only in configured time windows or time occasions. The time window/occasion configuration may be based on the DOA data transmission pattern of the target devices or device group. For example, if an AIoT sensor transmits data twice a day, say 5am in the morning and 11pm in the evening, the AIoT Readers assigned to collect the sensor data may be configured to monitor the sensor’s DRI broadcast in a time window around 5am and 11pm.

#### 6.16.1.2 Enhanced R19 AIoT Paging and Command procedures for collecting DOA data

Once the AIoT Reader monitors the DRI broadcast, the Reader may initiate an AIoT Paging procedure to handshake with the device that has data to send and verify the device identifier. The AIoT paging message needs to carry a DOA indication so that only the device(s) that has DOA data to send may respond to the paging. The Reader and the network will also determine the device identifier and verify it during this procedure.

After the device identifier is verified, the Reader may initiate a Read Command procedure to collect the data from the device.

#### 6.16.1.3 Routing of DOA data

When the AIoT Reader receives the DOA data from the AIoT device, it needs to forward it to the AIOTF which further forwards it to the AF. The determination of the AIOTF may be based on the Reader’s configuration that maps a part of device identifier to an AIOTF. For UE Readers, this configuration may also reside in the NG-RAN or AMF.

### 6.16.2 Procedures



Figure 6.16.2-1: DOA data detection and collection

1. The AIoT Reader monitors DRI broadcast on the preconfigured radio resource. If the Reader is a UE Reader, it may only monitor the DRI broadcast during the configured time windows which match the DOA data transmission pattern of the AIoT devices that the Reader is supposed to serve.

2. The AIoT device has DOA data ready to be sent. The device broadcasts a DRI signal on the preconfigured radio resource. This signal may be picked up by one or multiple Readers that monitor the DRI broadcast.

3. The AIoT Reader that detects the DRI signal may initiate the AIoT Paging towards the device. The Reader includes the DOA Indication in the Paging message, and there is no device identifier information in the Paging message.

4. The AIoT device that has DOA data to send receives the Paging message and sends the Paging Response message to the Reader. The Paging Response message includes the device’s identifier and may include other information, such as the approximate size of the DOA data to be sent.

Other AIoT devices that receive the Paging but don’t have DOA data to send should not respond to this Paging.

Editor's note: It is FFS how to handle the scenario that multiple AIoT Readers detect the DRI signal and send the AIoT Paging messages simultaneously.

NOTE 1: Step 2 – 4 are in the RAN WGs’ scope.

5. The AIoT Reader forwards the device identifier information to a selected AIOTF for the purpose of verifying the device identifier. The AIOTF may work with the ADM to verify the device identifier and return the result to the Reader. If the Reader is a UE Reader, the UE Reader forwards the information via NG-RAN and AIOTF to the AIOTF.

Editor's note: It is FFS how to verify the device identifier if it is a temporary identifier and it may need coordination with SA3.

6a/6b. If the device ID is successfully verified, the AIOTF initiates Read Command procedure via the AIoT Reader towards the device to collect the device’s DOA data.

7. The AIoT device sends the DOA data to the Reader in the Command Response message. Step 6 and 7 may repeat multiple times until all of the device’s DOA data is collected.

In case that only the designated Reader can handle the device’s DOA data, the device may also include a Reader Token that’s calculated from the preconfigured security credentials and inputs (e.g., designated Reader ID). The purpose of Reader Token is to prevent non-designated Readers from handling the data. If the Reader Token is included in the message, the Reader should calculate its own Reader Token and compare it with the received token. If the tokens match the Reader may continue to handle the data, otherwise, it should discard the data. The use of Reader Token is not related to the data encryption.

Editor's note: The use of Reader Token needs coordination with SA3.

8. The Reader selects the AIOTF for the DOA data using the local configuration that maps device identifier information to an AIOTF address. Note that this AIOTF may be different from the one that performs the device identifier verification in Step 5.

9. The Reader forwards the received DOA data to the selected AIOTF which further forwards it to the AF.

### 6.16.3 Impacts on Services, Entities and Interfaces

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

The proposed solution has impacts on the following entities:

AIoT Device:

- Support DRI signal generation and broadcast and related radio resource configuration.

- Support new “DOA Indication” in AIoT Paging message.

- Support Reader Token generation.

AIoT Reader:

- Support DRI signal monitoring and related radio resource configuration and time window configuration.

- Support Reader initiated Pagin and Command procedure (i.e., without receiving the Inventory/Command request from AIOTF).

- Support new “DOA Indication” in AIoT Paging message.

- Support AIOTF selection for routing DOA data to AIOTF and related configuration.

- Support Reader Token verification.

AIOTF:

- Support device identifier verification for DOA data.

- Support initiation of Command procedure.

- Support receiving DOA data from AIoT Readers and forward it to the AF.

## 6.17 Solution #17: Service aspects for DO-A traffic in Ambient IoT networks

### 6.17.1 High-level solution principles

The solution proposed in this paper is based on the following principles:

1. A new service type “DO-A support” for enabling DO-A traffic for a certain service within the network is introduced.

2. Network can simultaneously support devices that are capable of DO-A and DT traffic at the same time.

3. A-IoT readers present in the network can have varying capabilities. Some of them are able to support both DO-A and DT traffic, others can only support DT traffic.

4. DO-A capable devices can be configured by the network to support both DO-A traffic and DT traffic or only DT traffic at a given time.

This solution is applicable for scenarios when the NG-RAN expects an indication from the core network regarding DO-A service.

### 6.17.1 Description

For supporting DO-A traffic within an Ambient IoT network, an AF should first enable the service for supporting DO-A traffic within the network. This is essential as the AIoT Readers collocated with gNB (topology 1), or UE (topology 2) may need to broadcast certain specific signals for supporting DO-A traffic. These signals are used to typically allocate radio resource e.g., Random Access Channel (RACH) resources for enabling devices to access the network.

Enabling DO-A support as a service may help in energy saving in a twofold manner viz., 1). Energy Saving at the reader by reducing D2R signalling to support DO-A whenever DO-A capable devices are not present in the network or are disabled. 2) disabling a specific DO-A service for a device for supporting reduced energy consumption in the device.

Once DO-A service is enabled, a DO-A capable device(s) can register with the core network (AIOTF) with the service ID and is authenticated. It can then request for DO-A data transfer whenever it has some data to send.

### 6.17.2 Procedures

#### 6.17.2.1 Configuring the network to support DO-A support as a service

Figure 1 illustrates the call flow for enabling DO-A service in a AIoT Network.

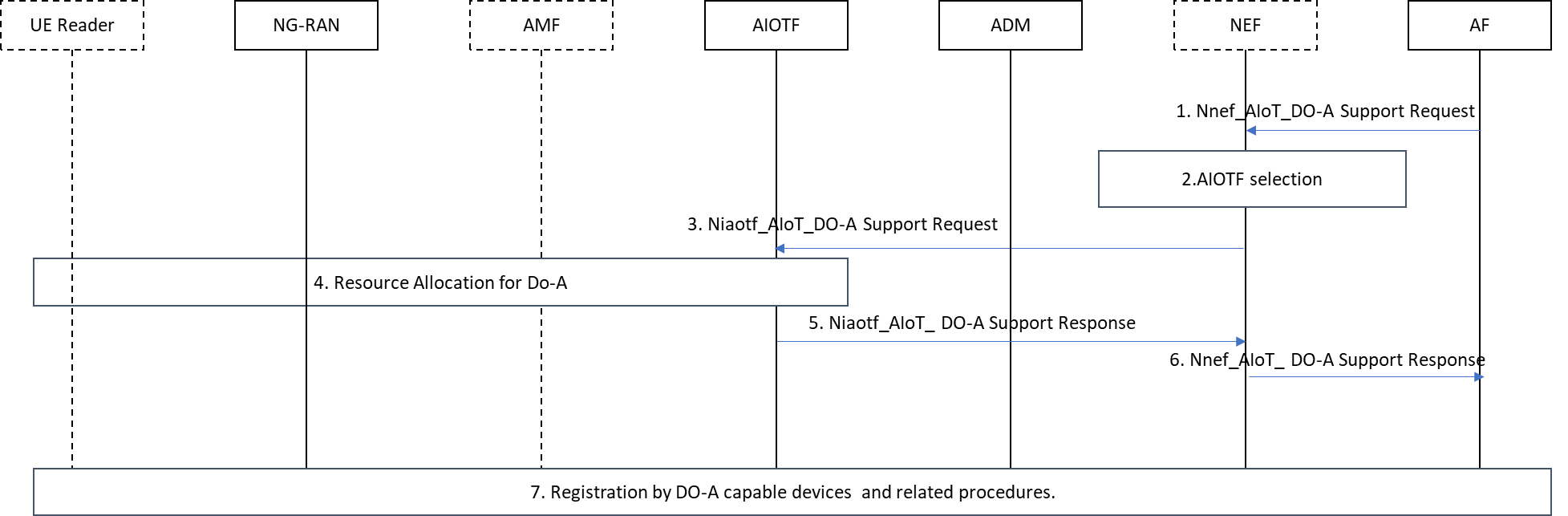


Figure 6.17.2.1-1:Procedure for supporting DO-A as a service.

The steps involved in the procedure are as follows:

1. The Application Function (AF) invokes Nnef\_AIoT\_Do-A Support (Service Descriptor, AF ID, [service type], [target area], operation, [priority] [list of device IDs] [offset][duration]) service operation request to the NEF. Service Descriptor is an identifier for every service request that arrives at the AF. It shall be unique within particular AF. The service descriptor that is sent as part of this service operation request shall be the descriptor of the service that needs to be enabled, modified or cancelled. AF ID is the identifier for a given AF. Service type in this request would correspond to “DO-A support”. Operation in this request could either enable or disable. The Priority field indicates the priority of the service request. The list of device IDs is an optional parameter in which the set of devices for which this service can be enabled/disabled is indicated. When not provided, the specified service is enabled for all the devices in the network. Similarly, offset and duration are optional parameters used for enabling/disabling a service at “offset” time interval from the point of receiving the request and “duration” is used to specify the duration of time for which the service remains enabled/disabled. When the duration is not provided, the service continues to stay enabled/disabled until a follow-up service request is issued.

NOTE 1: In case the AF is considered as a trusted AF, the AF may directly reach the AIOTF using the Naiotf\_AIoT\_Do-A Support Request (Service Descriptor, AF ID, [service type], [target area], operation, [priority] [list of device IDs] [offset][duration]).

2. The NEF may further authorize the AF request as specified in clause 5.6 of TS 23.369 [3]. The NEF determines the Target Area information and selects suitable AIOTF(s) that can support DO-A related traffic. The NEF determines AIOTF instances(s) by providing the NRF Target Area information along with the request for DO-A traffic support, and the NRF returning AIOTF instance(s) that match the Target Area information and ability to support DO-A, or by using local configuration. Once the NEF authorizes the AF request, the NEF creates a Transaction Reference ID for transferring this request to the AIOTF and stores the AF Identifier along with the Transaction Reference ID.

3. The NEF invokes Naiotf\_AIoT\_Do-A Support request (Transaction ID, AF ID, [service type], [target area], operation, [Approximate number of Do-A AIoT Devices], [Approximate number of AIoT Devices], [priority] [offset][duration]) towards to the selected AIOTF(s). The Approximate number of Do-A AIoT devices is an optional parameter and could be used for resource allocation.

4. AIOTF receives the Naiotf\_AIoT\_Do-A Support request and checks the parameters included in the request. The AIOTF may perform checks as specified in clause 5.6 of TS 23.369 [3]. Also, AIOTF may select a set of NG-RAN nodes and reader(s) within the target area for supporting DO-A traffic. The NG-RAN nodes and readers can be selected based on several criteria such as ability to support DO-A traffic, load on the NG-RAN nodes or readers, number of actively connected devices (both 5G NR UEs and A-IoT devices), available radio resources etc. The selected readers allocate radio resources for supporting DO-A traffic. For example, certain trigger time instants may be allocated to only support DO-A traffic from A-IoT devices. These resources may be broadcasted by the A-IoT readers or can be pre-configured by the network while the device is deployed. In case, the Naiotf\_AIoT\_Do-A Support request cannot be serviced due to any reason e.g., non-availability of readers supporting Rel-20, not enough resources etc., the AIOTF rejects the AIoT service operation request with an appropriate cause code in Step 5, and step 7 is skipped.

NOTE 2: The Naiotf\_AIoT\_Do-A Support is used to provide indication to the network that DO-A traffic may be expected within a certain time period. The necessity of this indication depends on RAN WGs.

5. AIOTF sends Naiotf\_AIoT\_Do-A Support Response to the NEF containing the accept or reject result for the Naiotf\_AIoT\_Do-A Support request based on step 4.

6. NEF sends Nnef\_AIoT\_Do-A Support Response to the AF, containing the accept or reject result for the AIoT service Cancel operation request as specified in clause 8.3 of TS 23.369 [3]. If the response was an accept, then DO-A enabled A-IoT devices are able to attempt successful registration with the network.

7. Any device capable of DO-A traffic support can now register with the network. Once registered with the network, it can initiate transmission of DO-A traffic whenever it has some data to transmit.

### 6.17.3 Impacts on Services, Entities and Interfaces

The following impacts are envisioned on the existing network functions:

AIOTF:

*-* For supporting DO-A traffic, AIOTF must support the mechanism to indicate to the Readers to enable any DO-A specific signalling.

ADM:

*-* The AIOTF profile data in the ADM must be enhanced to also contain “AIoT Device Traffic Capability” which can identify whether device can support DT only or both DT and DO-A traffic type. When DO-A traffic can be supported by the device, then it also maintains whether DO-A is enabled/disabled for the device for a given service. Similarly, AF Authorization Profile should indicate the support for DO-A for a specific service.

AF:

*-* For supporting DO-A, the functionality of AF is enhanced to enable or disable DO-A support for a specific service.

## 6.18 Solution #18: AIoT Device Registration and data transmission Procedure

### 6.18.0 High-level solution Principles

DO-A capable AIoT Devices have the ability to send MO originating signalling and data. The AIoT Device actively registers to the network to inform the network of its presence autonomously and once the AIoT Device is registered it can actively send data to the network autonomously without triggers from the network. The transferred data is included in AIoT NAS messages. The network is configured with a route for uplink data from the AIOT Device and the route is used when traffic is sent.

### 6.18.1 Description

This solution addresses KI#2, and includes how to enable the AIoT Device to inform the network of its presence autonomously for Topology 1, how to enable the device to perform DO-A data transmission, and Inventory and Command Procedures.

It is assumed that the AIoT Device actively initiates the registration process with the network and the data transmission procedure without any trigger from the network. The registration type can be an Initial Registration or a Mobility Registration Update when it to moves outside of an AIoT Registration Area. When an AIoT Device initially registers a context is created in the network for the AIoT Device and the AIoT Device is provided with an AIoT Registration Area.

Editor’s Note: It is FFS whether other registration type need to be supported.

AIoT Areas may span multiple Readers (and NG-RAN nodes) and a Reader may belong to multiple AIoT Areas. The granularity of the AIoT Areas and Readers can mean that the AIoT Device has to be provided with and store a large amount of information, or would have to perform Mobility Registration Updates frequently when the AIoT Device moves relatively small distances. While in some cases knowledge that the AIoT Device has moved a small distance is desirable, it is not a universal desire, and may cause significant overhead to AIoT Devices and networks.

Therefore, to enable the difference scenarios the network is configured with AIoT Registration Areas. An AIoT Registration Area is provided to the AIoT Device and is:

- A Reader list, AIoT tracking area code (TAC), or an AIoT Area List. The AIoT Device performs Mobility Registration Update if it moves outside of the list, TAC or AIoT Area List.

- Be hierarchical and be the first part of a TAC or a partial TAC. The AIoT Device performs Mobility Registration Update if the supplied part of the TAC no longer matches the TAC where the AIoT Device is.

The hierarchical AIoT Registration Area will reduce the amount of storage required by an AIoT Device.

NOTE 1: The AIoT Registration Area is specific to Ambient IoT and does not need to be aligned with registration areas used by an AMF for NR. The AIoT tracking area code (TAC) is a different type of area identification from an AIoT Area List.

An AIOTF can subscribe to events for AIoT Device mobility, similar to those supported in 5GS for UEs, to be informed when the AIoT Device moves outside of its AIoT Registration Area.

According to TS 23.369 [3] and TS 33.369 [11], the AIOTF is the supports termination point of the AIoT NAS protocol within the network, and supports the authentication of the AIoT Device. For a DO-A capable AIoT Devices the AIOTF remains the NAS termination point, including for device authentication, and additionally supports registration management and mobility management.

NOTE 2: The Temporary ID used in the procedures for AIoT Device identification and AIOTF selection will need alignment with SA3.

### 6.18.2 Procedures

#### 6.18.2.1 Registration Procedure

The Registration procedure is used by an AIoT Device for Initial Registration or a Mobility Registration Update when it to moves outside of an AIoT Registration Area provided to it.



Figure 6.15.2.1-1: Registration Procedure

1. The AIoT Device sends a D2R message to NG-RAN, including D2R parameters and a NAS Registration Request (Registration Type, device information, security parameters).

The D2R parameters contains, e.g., a Temporary ID (if available), the selected PLMN ID and allows NG-RAN to route the request to the appropriate AIOTF.

NOTE 1: The details of the D2R parameters need to be coordinated with RAN WG.

The Registration Type indicates if the AIoT Device is performing an Initial Registration or a Mobility Registration Update. The AIoT Device performs an Initial Registration if it is not registered with the network and performs a Mobility Registration if it has moved outside of its AIoT Registration Area.

2. NG-RAN selects an AIOTF based on the D2R parameters or local configuration and to send the NAS message received from the AIoT Device to. If Indirect Connectivity is used between NG-RAN and the AIOTF, NG-RAN sends the selected AIOTF ID to AMF which can then route the message to the selected AIOTF.

3. NG-RAN sends the Registration Request NAS Message, Temporary ID and selected PLMN ID from the D2R message, and Reader information to the selected AIOTF. If the Temporary ID indicates another AIOTF assigned it, the selected AIOTF fetches the AIoT Device context from that AIOTF.

4. [Conditional] The new AIOTF may determine an old AIOTF using the Temporary ID, and retrieves the AIoT Device context from the old AIOTF.

5. The AIOTF determines the ADM for the AIoT Device based on the AIoT Device’s permanent ID.

6. The AIOTF performs authentication and security procedures, and stores the security context.

NOTE 2: Details of authentication and security procedures will be determined by SA3 WG.

7. The AIOTF registers itself with ADM as serving AIOTF for the AIoT Device and may retrieve the subscription data for the AIoT Device.

8. [Conditional] The ADM informs the old AIOTF using Nadm\_SDM\_unsubscribe that it is no longer the serving AIOTF for the AIoT Device.

9. The AIOTF sends the Registration Accept to the AIoT Device, which may include a new Temporary ID and AIoT Registration Area.

NOTE 3: This solution does not provide any power consumption parameters, but if they are defined by other solutions, it is expected they can be supplied to the AIoT Device in this procedure, if required.

6.18.2.2 Configuration of MO data routing

The procedure to configure the routing of uplink traffic from an AIoT Device is show in figure 6.18.2.2-1.



Figure 6.18.2.2-1: DO-A Target AF information configuration Procedure

1. The AF sends an Nnef\_DOAconfiguration\_Create Request message (AIoT Device information, AF Identifier, validity time) to the NEF. The validity time is used to indicate the how long network maintains the DO-A configuration information. This subscribes the AF to notifications of received data, as described in clause 6.18.2.3.

2. The NEF selects an ADM based on the AIoT Device information received in step 1.

3. The NEF sends a Nadm\_DOAConfiguration\_Create Request message (AIoT Device information, AF Identifier, validity time) to the ADM.

4. The ADM validates the request from the NEF and stores the AF information for devices’ DO-A data transmission, i.e., AF Identifier and validity time.

5. The ADM sends the Nadm\_DOAConfiguration\_Create Response message to NEF to confirm the route has been stored.

6. The NEF sends Nnef\_DOAconfiguration\_Create Response to the AF to acknowledge acceptance of the Nnef\_DOAconfiguration\_Create Request.

#### 6.18.2.3 DO-A traffic routing

The procedure uses the routing information stored in the ADM to route DO-A traffic from an AIoT Device and is shown in figure 6.18.2.3-1.



Figure 6.18.2.3-1: DO-A Data Transmission Procedure

1. The AIoT Device sends D2R message to NG-RAN, including Temporary ID and AIoT UL NAS message (Temporary ID, DO-A Data).

2. Based on the Temporary ID, NG-RAN selects an AIOTF, and forwards the AIoT UL NAS message and the RAN AIoT Device NGAP ID to the selected AIOTF. If Indirect Connectivity is used between NG-RAN and the AIOTF, NG-RAN sends the selected AIOTF ID to AMF so it can route the messages to the AIOTF. The AIoT Device may provide NG-RAN with an indication that follow on NAS message(s) to or from the AIoT Device or AIOTF are expected. When NG-RAN receives a follow-on indication, it can ensure that subsequent messages can be sent from the AIoT Device.

3. The AIOTF obtains the target AF information for the AIoT Device through subscribing to the ADM.

4. The AIOTF forwards the AIoT Device ID, DO-A Data and the target AF information an NEF. The NEF does not have to be the same NEF that that AF used to provide the routing information to the network.

5. The NEF forwards the AIoT Device ID, DO-A Data to the AF based on the target AF information.

#### 6.18.2.4 Inventory Procedures

The Inventory Procedure as specified in TS 23.369 [3], clause 6.2.2 is performed with following differences:

- In step 2, if the information about the target AIoT Device(s) has been provided, the NEF determines the corresponding serving AIOTFs by querying the ADM for the serving AIOTF based on the AIoT Device ID, and uses that AIOTF to perform the Inventory Procedure.

- In step 11, the AIOTF may find the serving AIOTF based on the Temporary ID, and retrieve the AIoT Device ID from the serving AIOTF. The AIoT Device context is not transferred, therefore a new Temporary ID does not need to be provided to the AIoT Device.

NOTE: Power consumption parameters might need to be provided to NG-RAN when performing the Inventory Procedure, and details are expected to described other solutions.

#### 6.18.2.5 Command Procedures

The Command Procedure as specified in TS 23.369 [3], clause 6.2.3 is performed with following differences:

- In step 2, if the information about the target AIoT Device(s) has been provided, the NEF determines the corresponding serving AIOTFs by querying the ADM for the serving AIOTF based on the AIoT Device ID, and uses that AIOTF to perform inventory procedure.

- In step 7, the AIOTF may find the serving AIOTF based on routing information, e.g., from within the temporary ID, and fetch AIoT Device contexts from the serving AIOTFs. It also registers/updates itself in the ADM as new Serving AIOTF.

If the serving AIOTF has changed, a new Temporary ID, needs be generated and provided to the AIoT Device so when it performs DO-A procedure the new AIOTF can be selected by NG-RAN.

- In step 8, the new Temporary ID, is provided to the AIoT Device along with the NAS Command Request message.

NOTE: Power consumption parameters might need to be provided to NG-RAN when performing the Command Procedure, and details are expected to described other solutions.

### 6.18.3 Impacts on Services, Entities and Interfaces

**AIOTF:**

- Support Registration and Mobility Management.

- Support DO-A data routing, including retrieval of AF Identifier from ADM

- Register AIOTF ID into ADM as serving AIOTF of the AIoT Device

**NG-RAN:**

- Supports AIOTF selection and transferring NAS messages to and from the AIoT Device.

**AIoT Device:**

- Support performing registration procedure.

**ADM:**

- Support storage of AIOTF ID as serving AIOTF for AIoT Device.

- Support storage of AF Identifier for AIoT Device

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

### 6.X.0 High-level solution Principles

Editor's note: Where possible similar/overlapping solution proposals should be documented as a single solution in the TR.

Documentation of more than one solution from the same company for the same KI is allowed but it shouldn't be expected that all of them will be documented in the TR.

### 6.X.1 Description

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

### 6.X.2 Procedures

Editor's note: This clause will describe the 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 Interim agreements

## 7.1 Agreed Principles

### 7.1.1 Agreed Principles for KI#1

Figure 7.1.1-1 depicts the AIoT System Architecture for Topology 2.

****

Figure 7.1.1-1: AIoT System Architecture for Topology 2

Figure 7.1.1-2 depicts the AIoT system architecture, using the reference point representation.

****

Figure 7.1.1-2: AIoT System Architecture for Topology 2 in reference point representation

NOTE: Whether the interface between AIOTF and UDM is needed will be checked in later phase.

**Message and protocol stack**

- Messages between the UE Reader and the AIOTF are delivered using RRC between UE and NG-RAN and NGAP between NG-RAN and AMF, and using an SBI interface between AMF and AIOTF. The related protocol stack is shown in Figure 7.1.1-3.



**Figure 7.1.1-3: Protocol Stack for the RRC option**

**UE reader authorization and revocation part:**

**- Subscription aspects:**

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

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

Editor’s note: Whether and what additional subscription information for the UE Reader is needed is FFS.

- UE Reader subscription information is available to AMF.

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

Editor’s note: Whether to inform the UE about the authorization information is FFS.

Editor’s note: Whether UE reader capability is provided to AMF is FFS.

- If the subscription information has been revoked, the indication that the UE is not authorized to operate as a UE Reader from the UDM, then the AMF informs NG-RAN that the UE is not authorized to operate as a UE Reader.

Editor’s note: Whether and how UE Reader subscription information is provided to AIOTF is FFS.

**- Radio resource management for UE Reader operation:**

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

**AIOTF Discovery and Selection for UE reader ID:**

Editor’s note: How to discover and select AIOTF when AF provides UE reader ID is FFS.

**UE reader selection part:**

Two scenarios will be supported for UE reader selection, AF providing UE reader ID case and AF providing Area case for all types of UE reader.

- For AF providing UE reader ID case:

- If UE Reader ID(s) is provided by the AF via the NEF for the operation, then that is used as the selected Reader(s) if authorized as UE reader. The AIOTF provides the selected UE Reader(s) to the NG-RAN.

Editor’s note: How to select UE reader(s) based on the AF provided area information is FFS.

**UE reader ID allocation:**

Editor’s note: Whether and how to allocate the UE reader ID is FFS.

## 7.2 Topics for further consideration

### 7.2.Z Topics for further consideration for KI#Z

Editor's note: This clause will include the topics for further consideration as work progresses for the specific KI#Z. Eventually this clause should only contain topics for further consideration that did not result in agreements (i.e. in agreed principle(s) in a clause 7.1.Z) and can either be then marked as not pursued or postponed to a future release.

# 8 Conclusions

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

Where there is consensus, interim agreements (e.g. solution principles descriptions) should be documented in the TR as soon as possible during a study.

These can be documented in the TR as "7.1.Y Agreed Principles for KI#Y" in the "Interim Agreements" clause. If the interim agreement has impacts on another clause in the TR and if there is consensus, that TR clause can be updated.

By consensus interim agreements can become part of the final conclusions of the study.

The Overall Evaluation clause previously used in TR skeletons should not be used.

There should be a Topics for further consideration clause per Key Issue. It is recommended that this is used e.g. to capture common issues that need to be resolved for multiple solutions.

Annex A:  
Change History

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA2#170 | S2-2506350 | - | - | - | Proposed skeleton agreed at SA2#170 | 0.0.0 |
| 2025-08 | SA2#170 |  | - | - | - | Inclusion of documents approved in SA2#170:  S2-2507706, S2-2507707, S2-2507761, S2-2507764,S2-2507765, S2-2507766, S2-2507767, S2-2507796, S2-2507797 | 0.1.0 |
| 2025-10 | SA2#171 |  | - | - | - | Inclusion of documents approved in SA2#171:  S2-2509386, [S2-2509387](E:\\3GPP会议\\SA2\\SA2#171_Wuhan25\\Agreed_AIoT_PCRs\\Docs\\S2-2509387.zip), S2-2509405, S2-2509407, S2-2509409, S2-2509411, S2-2509450, S2-2509451, S2-2509453, S2-2509454, S2-2509455, S2-2509456, S2-2509459, S2-2509658, S2-2509829 | 0.2.0 |