

# ETSI TS 129 369 V19.0.0 (2026-01)



TECHNICAL SPECIFICATION

**5G;  
5G System;  
Ambient IoT Data Management Services;  
Stage 3  
(3GPP TS 29.369 version 19.0.0 Release 19)**



---

Reference

DTS/TSGC-0429369vj00

---

Keywords

5G

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at [3GPP to ETSI numbering cross-referencing](#).

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

Intellectual Property Rights .....	2
Legal Notice .....	2
Modal verbs terminology.....	2
Foreword.....	5
1 Scope .....	7
2 References .....	7
3 Definitions and abbreviations.....	8
3.1 Definitions .....	8
3.2 Abbreviations .....	8
4 Overview .....	8
5 Services offered by the ADM.....	8
5.1 Introduction .....	8
5.2 Nadm_DM Service.....	9
5.2.1 Service Description.....	9
5.2.2 Service Operations .....	9
5.2.2.1 Introduction.....	9
5.2.2.2 Query.....	9
5.2.2.2.1 General .....	9
5.2.2.2.2 AIoT Device Profile Data Retrieval .....	9
5.2.2.2.3 AF Authorization Data Retrieval.....	10
5.2.2.3 Update .....	10
5.2.2.3.1 AIoT Device Profile Data Update .....	10
6 API Definitions .....	11
6.1 Nadm_DM Service API .....	11
6.1.1 Introduction.....	11
6.1.2 Usage of HTTP .....	11
6.1.2.1 General .....	11
6.1.2.2 HTTP standard headers .....	11
6.1.2.2.1 General .....	11
6.1.2.2.2 Content type .....	11
6.1.2.3 HTTP custom headers .....	12
6.1.3 Resources.....	12
6.1.3.1 Overview.....	12
6.1.3.2 Resource: AiotDeviceProfileData .....	12
6.1.3.2.1 Description .....	12
6.1.3.2.2 Resource Definition.....	13
6.1.3.2.3 Resource Standard Methods .....	13
6.1.3.3 Resource: AfAuthorizationData.....	14
6.1.3.3.1 Description .....	14
6.1.3.3.2 Resource Definition.....	14
6.1.3.3.3 Resource Standard Methods .....	15
6.1.4 Custom Operations without associated resources .....	16
6.1.5 Notifications .....	16
6.1.6 Data Model .....	16
6.1.6.1 General .....	16
6.1.6.2 Structured data types .....	17
6.1.6.2.1 Introduction .....	17
6.1.6.2.2 Type: AiotDevProfileData.....	17
6.1.6.2.3 Type: LastKnownAiotfInfo .....	17
6.1.6.2.4 Type: IndividualAfAuthorizationData.....	18
6.1.6.2.5 Type: AllowedTargetAiotDevice .....	18
6.1.6.2.6 Type: AfAuthorizationData .....	18

6.1.6.3	Simple data types and enumerations .....	19
6.1.6.3.1	Introduction .....	19
6.1.6.3.2	Simple data types.....	19
6.1.6.3.3	Enumeration: AllowedServiceOperation.....	19
6.1.7	Error Handling .....	19
6.1.7.1	General .....	19
6.1.7.2	Protocol Errors .....	19
6.1.7.3	Application Errors.....	19
6.1.8	Feature negotiation .....	19
6.1.9	Security .....	20
6.1.10	HTTP redirection .....	20
<b>Annex A (normative):</b>	<b>OpenAPI specification.....</b>	<b>21</b>
A.1	General .....	21
A.2	Nadm_DM API .....	21
<b>Annex B (informative):</b>	<b>Change history .....</b>	<b>26</b>
History .....		27

---

# Foreword

This Technical Specification 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 specifies the stage 3 protocol and data model for the Nadm Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the ADM.

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.369[14].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in 3GPP TS 29.500 [4] and 3GPP TS 29.501 [5].

---

# 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 23.501: "System Architecture for the 5G System; Stage 2".
- [3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".
- [4] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".
- [5] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".
- [6] OpenAPI: "OpenAPI Specification Version 3.0.0", <https://spec.openapis.org/oas/v3.0.0>.
- [7] 3GPP TR 21.900: "Technical Specification Group working methods".
- [8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".
- [9] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".
- [10] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".
- [11] IETF RFC 9113: "HTTP/2".
- [12] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".
- [13] IETF RFC 9457: "Problem Details for HTTP APIs".
- [14] 3GPP TS 23.369: " Architecture support for Ambient power-enabled Internet of Things; Stage 2".
- [15] IETF RFC 9110: "http Semantics".
- [16] IETF RFC 9111: "HTTP Caching".
- [17] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and 3GPP TS 23.369 [14] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

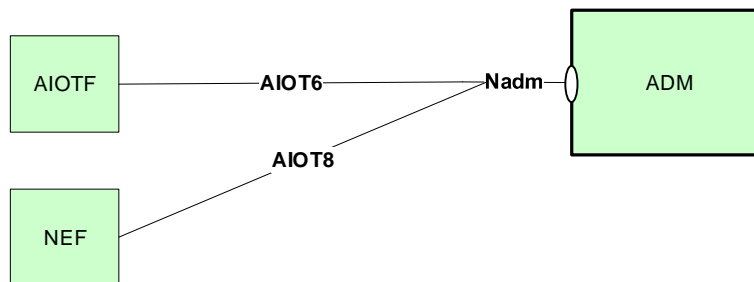
### 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and 3GPP TS 23.369 [14] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

## 4 Overview

Within the 5GC, the ADM offers services to the AIOTF, NEF via the Nadm service based interface (see 3GPP TS 23.369 [14]).

Figure 4-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the ADM:



**Figure 4-1: Reference model – ADM**

The functionalities supported by the ADM are listed in clause 4.5.9 of 3GPP TS 23.369 [14].

## 5 Services offered by the ADM

### 5.1 Introduction

The ADM offers the following services via the Nadm interface:

- Nadm\_DM Service

Table 5.1-1 summarizes the corresponding APIs defined for this specification.

**Table 5.1-1: API Descriptions**

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Nadm_DM	6.1	ADM Data Management	TS29369_Nadm_DM.yaml	nadm-dm	A.2

## 5.2 Nadm\_DM Service

### 5.2.1 Service Description

The Nadm\_DM service enables an NF to request AIoT device profile data or the AF authorization data or update the AIoT device profile data in the ADM.

### 5.2.2 Service Operations

#### 5.2.2.1 Introduction

The service operations defined for the Nadm\_DM service are as follows:

- Query: It enables a consumer NF to request AIoT device profile data or the AF authorization data from the ADM.
- Update: It enables a consumer NF to update the AIoT device profile data in the ADM.

#### 5.2.2.2 Query

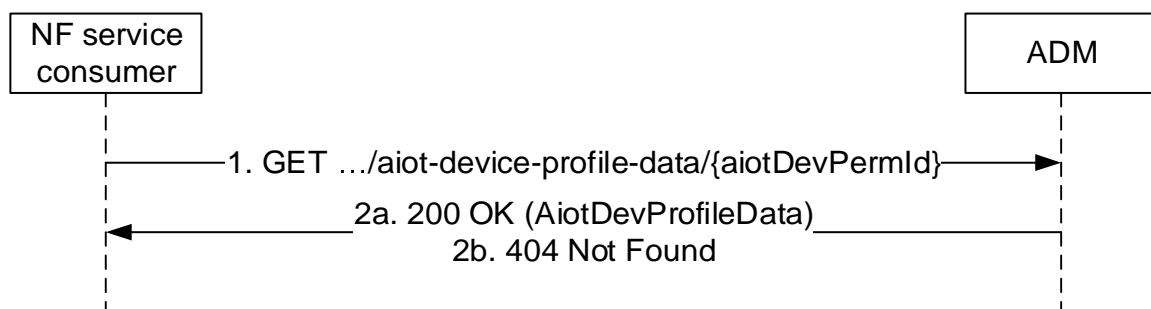
##### 5.2.2.2.1 General

The following procedures using the Query service operation are supported:

- AIoT Device Profile Data Retrieval
- AF Authorization Data Retrieval

##### 5.2.2.2.2 AIoT Device Profile Data Retrieval

Figure 5.2.2.2.2-1 shows a scenario where the NF service consumer (e.g. AIOTF or NEF) sends a request to the ADM to receive the AIoT Device Profile Data (see 3GPP TS 23.369 [14]).



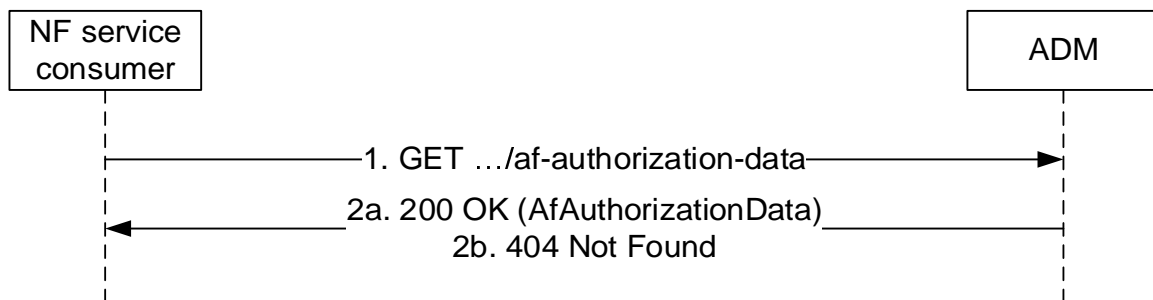
**Figure 5.2.2.2.2-1: Requesting AIoT Device Profile Data**

1. The NF service consumer (e.g. AIOTF or NEF) sends a GET request to the resource `.../aiot-device-profile-data/{aiotDevPermId}`, to get the AIoT Device Profile Data.
- 2a. On success, the ADM responds with "200 OK" with the AIoT Device Profile Data.
- 2b. If there is no valid AIoT Device Profile Data for the AIoT device permanent identifier, HTTP status code "404 Not Found" shall be returned including additional error information in the response body (in the "ProblemDetails" element).

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the GET response body.

### 5.2.2.2.3 AF Authorization Data Retrieval

Figure 5.2.2.2.3-1 shows a scenario where the NF service consumer (e.g. AIOTF, NEF) sends a request to the ADM to receive the AF Authorization Data (see 3GPP TS 23.369 [14]).



**Figure 5.2.2.2.3-1: Requesting AF Authorization Data**

1. The NF service consumer (e.g. AIOTF, NEF) sends a GET request to the resource of the AF authorization data (.../af-authorization-data), to get the Authorization Data of the AFs. The request may contain the target AF ID if the authorization data for a specific AF is to be retrieved.
- 2a. On success, the ADM responds with "200 OK" with the Authorization Data of the target AF(s).
- 2b. If there is no valid AF Authorization Data available, HTTP status code "404 Not Found" shall be returned including additional error information in the response body (in the "ProblemDetails" element).

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the GET response body.

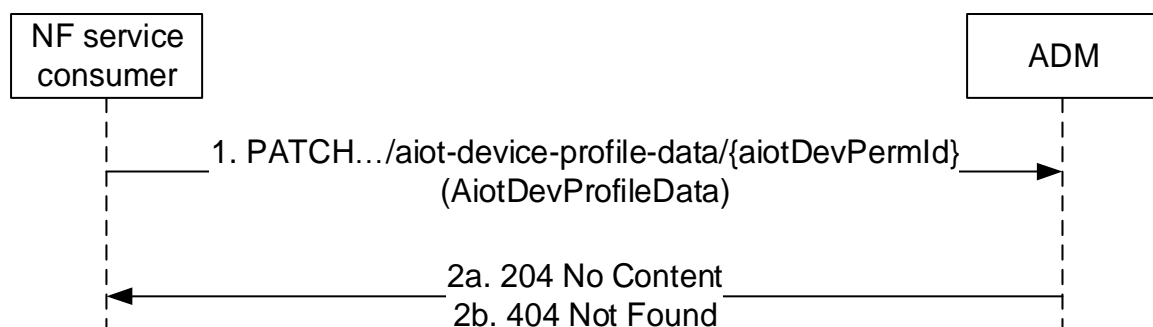
### 5.2.2.3 Update

The following procedures using the Update service operation are supported:

- AIoT Device Profile Data Update

#### 5.2.2.3.1 AIoT Device Profile Data Update

Figure 5.2.2.3.1-1 shows a scenario where the NF service consumer (e.g., AIOTF) sends a request to the ADM to modify the AIoT Device Profile Data (see 3GPP TS 23.369 [14]). The request contains the AIoT device permanent identifier and the modification instructions.



**Figure 5.2.2.3.1-1: Updating AIoT Device Profile Data**

1. The NF service consumer (e.g. AIOTF) sends a PATCH request to the resource .../aiot-device-profile-data/{aiotDevPermId}, to update the AIoT Device Profile Data.
- 2a. On success, the ADM responds with "204 No Content".

2b. If there is no valid AIoT Device Profile Data for the AIoT device permanent identifier, HTTP status code "404 Not Found" shall be returned including additional error information in the response body (in the "ProblemDetails" element).

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the PATCH response body.

---

## 6 API Definitions

### 6.1 Nadm\_DM Service API

#### 6.1.1 Introduction

The Nadm\_DM shall use the Nadm\_DM API.

The API URI of the Nadm\_DM API shall be:

**{apiRoot}/<apiName>/<apiVersion>**

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [5], i.e.:

**{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>**

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].
- The <apiName> shall be "nadm-dm".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.1.3.

#### 6.1.2 Usage of HTTP

##### 6.1.2.1 General

HTTP/2, IETF RFC 9113 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [6] specification of HTTP messages and content bodies for the Nadm\_DM API is contained in Annex A.

##### 6.1.2.2 HTTP standard headers

###### 6.1.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

###### 6.1.2.2.2 Content type

JSON, IETF RFC 8259 [12], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 9457 [13].

### 6.1.2.3 HTTP custom headers

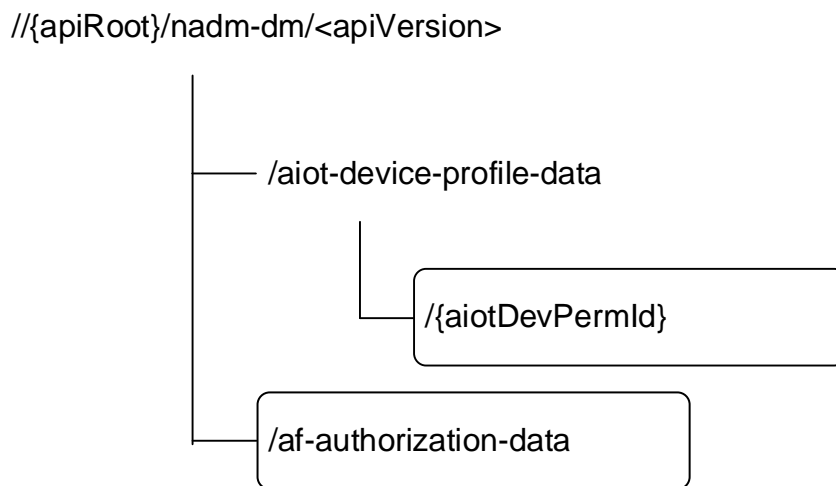
The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

## 6.1.3 Resources

### 6.1.3.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 6.1.3.1-1 depicts the resource URIs structure for the Nadm\_DM API.



**Figure 6.1.3.1-1: Resource URI structure of the Nadm\_DM API**

Table 6.1.3.1-1 provides an overview of the resources and applicable HTTP methods.

**Table 6.1.3.1-1: Resources and methods overview**

Resource purpose/name	Resource URI (relative path after API URI)	HTTP method or custom operation	Description (service operation)
AiotDeviceProfileData	/aiot-device-profile-data/{aiotDevPerId}	GET	Retrieve AIoT Device Profile Data
		PATCH	Modify AIoT Device ProfileData
AfAuthorizationData	/af-authorization-data	GET	Retrieve AF Authorization Data

### 6.1.3.2 Resource: AiotDeviceProfileData

#### 6.1.3.2.1 Description

This resource is used to represent AIoT Device Profile Data.

## 6.1.3.2.2 Resource Definition

Resource URI: {apiRoot}/nadm-dm/<apiVersion>/aiot-device-profile-data/{aiotDevPermId}

This resource shall support the resource URI variables defined in table 6.1.3.2.2-1.

**Table 6.1.3.2.2-1: Resource URI variables for this resource**

Name	Data type	Definition
apiRoot	string	See clause 6.1.1
aiotDevPermId	AiotDevPermId	Represents the AIoT Device Permanent ID (see 3GPP TS 23.369 [14] clause 5.7.2)

## 6.1.3.2.3 Resource Standard Methods

## 6.1.3.2.3.1 GET

This method shall support the URI query parameters specified in table 6.1.3.2.3.1-1.

**Table 6.1.3.2.3.1-1: URI query parameters supported by the GET method on this resource**

Name	Data type	P	Cardinality	Description	Applicability
n/a					

This method shall support the request data structures specified in table 6.1.3.2.3.1-2 and the response data structures and response codes specified in table 6.1.3.2.3.1-3.

**Table 6.1.3.2.3.1-2: Data structures supported by the GET Request Body on this resource**

Data type	P	Cardinality	Description
n/a			

**Table 6.1.3.2.3.1-3: Data structures supported by the GET Response Body on this resource**

Data type	P	Cardinality	Response codes	Description
AiotDevProfileData	M	1	200 OK	Upon success, a response body containing the AIoT Device Profile Data shall be returned.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - DATA_NOT_FOUND
NOTE: The mandatory HTTP error status code for the GET method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

**Table 6.1.3.2.3.1-4: Headers supported by the GET method on this resource**

Name	Data type	P	Cardinality	Description
If-None-Match	string	O	0..1	Validator for conditional requests, as described in IETF RFC 9110 [15], clause 13.1.2
If-Modified-Since	string	O	0..1	Validator for conditional requests, as described in IETF RFC 9110 [15], clause 13.1.3

**Table 6.1.3.2.3.1-5: Headers supported by the 200 response code on this resource**

Name	Data type	P	Cardinality	Description
Cache-Control	string	O	0..1	Cache-Control containing max-age, as described in IETF RFC 9111 [16], clause 5.2
ETag	string	O	0..1	Entity Tag, containing a strong validator, as described in IETF RFC 9110 [15], clause 8.8.3
Last-Modified	string	O	0..1	Timestamp for last modification of the resource, as described in IETF RFC 9110 [15], clause 8.8.2

### 6.1.3.2.3.2 PATCH

This method shall support the URI query parameters specified in table 6.1.3.2.3.2-1.

**Table 6.1.3.2.3.2-1: URI query parameters supported by the PATCH method on this resource**

Name	Data type	P	Cardinality	Description
supported-features	SupportedFeatures	O	0..1	see 3GPP TS 29.500 [4] clause 6.6

This method shall support the request data structures specified in table 6.1.3.2.3.2-2 and the response data structures and response codes specified in table 6.1.3.2.3.2-3.

**Table 6.1.3.2.3.2-2: Data structures supported by the PATCH Request Body on this resource**

Data type	P	Cardinality	Description
AiotDevProfileData	M	1	Contains the updated AIoT Device Profile Data

**Table 6.1.3.2.3.2-3: Data structures supported by the PATCH Response Body on this resource**

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Upon success, an empty response body shall be returned. (NOTE 2)
PatchResult	M	1	200 OK	Upon success, the execution report is returned. (NOTE 2)
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - DATA_NOT_FOUND
NOTE 1: In addition common data structures as listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] are supported.				
NOTE 2: If all the modification instructions in the PATCH request have been implemented, the ADM shall respond with 204 No Content response; if some of the modification instructions in the PATCH request have been discarded, and the NF service consumer has included in the supported-feature query parameter the "PatchReport" feature number, the ADM shall respond with PatchResult.				

## 6.1.3.3 Resource: AfAuthorizationData

### 6.1.3.3.1 Description

This resource is used to represent AF Authorization Data.

### 6.1.3.3.2 Resource Definition

Resource URI: {apiRoot}/nadm-dm/<apiVersion>/af-authorization-data

This resource shall support the resource URI variables defined in table 6.1.3.3.2-1.

**Table 6.1.3.3.2-1: Resource URI variables for this resource**

Name	Data type	Definition
apiRoot	string	See clause 6.1.1

### 6.1.3.3.3 Resource Standard Methods

#### 6.1.3.3.3.1 GET

This method shall support the URI query parameters specified in table 6.1.3.3.3.1-1.

**Table 6.1.3.3.3.1-1: URI query parameters supported by the GET method on this resource**

Name	Data type	P	Cardinality	Description	Applicability
af-id	Afid	O	0..1	When present, this parameter indicates the AF for whom the Authorization data is to be retrieved.  When this IE is absent, it shall indicate that the Authorization Data for all the AFs are to be retrieved.	

This method shall support the request data structures specified in table 6.1.3.3.3.1-2 and the response data structures and response codes specified in table 6.1.3.3.3.1-3.

**Table 6.1.3.3.3.1-2: Data structures supported by the GET Request Body on this resource**

Data type	P	Cardinality	Description
n/a			

**Table 6.1.3.3.3.1-3: Data structures supported by the GET Response Body on this resource**

Data type	P	Cardinality	Response codes	Description
AfAuthorizationData	M	1	200 OK	Upon success, a response body containing the AF Authorization Data shall be returned.
ProblemDetails	O	0..1	404 Not Found	The "cause" attribute may be used to indicate one of the following application errors: - DATA_NOT_FOUND
NOTE: The mandatory HTTP error status code for the GET method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

**Table 6.1.3.3.3.1-4: Headers supported by the GET method on this resource**

Name	Data type	P	Cardinality	Description
If-None-Match	string	O	0..1	Validator for conditional requests, as described in IETF RFC 9110 [15], clause 13.1.2
If-Modified-Since	string	O	0..1	Validator for conditional requests, as described in IETF RFC 9110 [15], clause 13.1.3

**Table 6.1.3.3.1-5: Headers supported by the 200 response code on this resource**

Name	Data type	P	Cardinality	Description
Cache-Control	string	O	0..1	Cache-Control containing max-age, as described in IETF RFC 9111 [16], clause 5.2
ETag	string	O	0..1	Entity Tag, containing a strong validator, as described in IETF RFC 9110 [15], clause 8.8.3
Last-Modified	string	O	0..1	Timestamp for last modification of the resource, as described in IETF RFC 9110 [15], clause 8.8.2

## 6.1.4 Custom Operations without associated resources

In this release of this specification, no custom operations without associated resources are defined for the Nadm\_DM Service.

## 6.1.5 Notifications

In this release of this specification, no notifications are defined for the Nadm\_DM Service.

## 6.1.6 Data Model

### 6.1.6.1 General

This clause specifies the application data model supported by the API.

Table 6.1.6.1-1 specifies the data types defined for the Nadm\_DM service based interface protocol.

**Table 6.1.6.1-1: Nadm\_DM specific Data Types**

Data type	Clause defined	Description	Applicability
AiotDevProfileData	6.1.6.2.2	AIoT Device Profile Data	
LastKnownAiotfInfo	6.1.6.2.3	Last Known AIoTF Information	
IndividualAfAuthorizationData	6.1.6.2.4	Individual AF Authorization Data	
AllowedTargetAiotDevice	6.1.6.2.5	Allowed Target AIoT Device	
AfAuthorizationData	6.1.6.2.6	AF Authorization Data	
LastKnownAiotfInfoInd	6.1.6.3.2	Last known AIoTF Information	
Afid	6.1.6.3.2	AF ID	
AllowedServiceOperation	6.1.6.3.3	Allowed Service Operation	

Table 6.1.6.1-2 specifies data types re-used by the Nadm\_DM service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nadm\_DM service based interface.

**Table 6.1.6.1-2: Nadm\_DM re-used Data Types**

Data type	Reference	Comments	Applicability
SupportedFeatures	3GPP TS 29.571 [17]	see 3GPP TS 29.500 [4] clause 6.6	SupportedFeatures
AiotDevPermId	3GPP TS 29.571 [17]	AIoT device permanent identifier	
AiotArea	3GPP TS 29.571 [17]	Contains the AIoT Area	
NfInstancelId	3GPP TS 29.571 [17]	Represent a NF instance.	
IpAddr	3GPP TS 29.571 [17]	Represent the IP address	
Fqdn	3GPP TS 29.571 [17]	Represent Fully Qualified Domain Name	
ProblemDetails	3GPP TS 29.571 [17]	Used in error responses to provide more detailed information about an error.	

## 6.1.6.2 Structured data types

### 6.1.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

#### 6.1.6.2.2 Type: AiotDevProfileData

**Table 6.1.6.2.2-1: Definition of type AiotDevProfileData**

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevPerMId	AiotDevPerMId	M	1	Globally unique AIoT device permanent identifier	
lastKnownAiotfInfo	LastKnownAiotfInfo	M	1	Indicate the last known AIOTF that serves the AIoT device, or unknown.	

#### 6.1.6.2.3 Type: LastKnownAiotfInfo

**Table 6.1.6.2.3-1: Definition of type LastKnownAiotfInfo**

Attribute name	Data type	P	Cardinality	Description	Applicability
lastKnownAiotfInfoInd	boolean	M	1	Indicate the last known AIOTF that serves the AIoT device is known, or unknown. true: Known; false: Unknown	
lastKnownAiotfId	NfInstanceId	C	0..1	This IE may be present when lastKnownAiotfInfoInd is set to true. Indicates the last known AIOTF instance (NOTE)	
lastKnownAiotfAddress	IpAddr	C	0..1	This IE may be present when lastKnownAiotfInfoInd is set to true. Indicates the IP address for last known AIOTF instance (NOTE)	
lastKnownAiotfFqdn	Fqdn	C	0..1	This IE may be present when lastKnownAiotfInfoInd is set to true. Indicates the FQDN for last known AIOTF instance (NOTE)	
NOTE: At least, one of lastKnownAiotfId, lastKnownAiotfAddress and lastKnownAiotfFqdn shall be included when lastKnownAiotfInfoInd is set to true.					

## 6.1.6.2.4 Type: IndividualAfAuthorizationData

**Table 6.1.6.2.4-1: Definition of type IndividualAfAuthorizationData**

Attribute name	Data type	P	Cardinality	Description	Applicability
afId	AfId	M	1	Identifier used to identify the AF.	
allowedArea	AiotArea	C	0..1	If present, it indicates the allowed area for the indicated AF to perform the AIoT services operations.  If this attribute is absent, it means that the complete service area is allowed for the AF.	
allowedServiceOperations	array(AllowedServiceOperation)	C	1..N	If present, it indicates the list of allowed service operation(s) for the AF.  If this attribute is absent, it means that all the Service Operations are allowed for the AF.	
allowedTargetAiotDevices	array(AllowedTargetAiotDevice)	C	1..N	If present, it indicates the list of allowed AIoT Device(s) for the AF.  If this attribute is absent, it means that all the Target Aiot Devices are allowed for the AF.	

## 6.1.6.2.5 Type: AllowedTargetAiotDevice

**Table 6.1.6.2.5-1: Definition of type AllowedTargetAiotDevice**

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevPermId	AiotDevPermId	O	0..1	Indicates the AIoT Device Permanent ID. (NOTE)	
filteringInfo	AiotFilteringInformation	O	0..1	Indicates the Filtering Information. (NOTE)	
NOTE: Either aiotDevPermId, or filteringInfo shall be present.					

## 6.1.6.2.6 Type: AfAuthorizationData

**Table 6.1.6.2.6-1: Definition of type AfAuthorizationData**

Attribute name	Data type	P	Cardinality	Description	Applicability
afAuthData	map(IndividualAfAuthorizationData)	M	1..N	A map contains the AF Authorization Data in the ADM. The key of the map is the AF ID and the value of the map is the Authorization data of the corresponding AF indicated by the key.	

### 6.1.6.3 Simple data types and enumerations

#### 6.1.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

#### 6.1.6.3.2 Simple data types

The simple data types defined in table 6.1.6.3.2-1 shall be supported.

**Table 6.1.6.3.2-1: Simple data types**

Type Name	Type Definition	Description	Applicability
AfId	string	Identifier used to identify the AF.	

#### 6.1.6.3.3 Enumeration: AllowedServiceOperation

The enumeration AllowedServiceOperation represents the different types of the allowed service operation for the AF.

**Table 6.1.6.3.3-1: Enumeration AllowedServiceOperation**

Enumeration value	Description	Applicability
"INVENTORY"	Indicates inventory service operation is allowed for the AF.	
"READ"	Indicates read service operation is allowed for the AF.	
"WRITE"	Indicates write service operation is allowed for the AF.	
"PERMANENT_DISABLE"	Indicates permanent disable service operation is allowed for the AF.	

### 6.1.7 Error Handling

#### 6.1.7.1 General

HTTP error handling shall be supported as specified in clause 5.2.4 of 3GPP TS 29.500 [4].

#### 6.1.7.2 Protocol Errors

Protocol errors handling shall be supported as specified in clause 5.2.7 of 3GPP TS 29.500 [4].

#### 6.1.7.3 Application Errors

The common application errors defined in Table 5.2.7.2-1 in 3GPP TS 29.500 [4] may be used for the Nadm\_DM. The application errors defined for the Nadm\_DM service are listed in Table 6.1.7.3-1.

**Table 6.1.7.3-1: Application errors**

Application Error	HTTP status code	Description
DATA_NOT_FOUND	404 Not Found	The requested AIoT Device Profile Data or AF Authorization Data is not found/does not exist.

### 6.1.8 Feature negotiation

The optional features in table 6.1.8-1 are defined for the Nadm\_DM API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

**Table 6.1.8-1: Supported Features**

Feature number	Feature Name	Description

## 6.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the <API Name> API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the <API Name> API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], clause 5.4.2.2.

**NOTE:** When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the <API Name> service.

The Nadm\_DM API defines the following scopes for OAuth2 authorization.

**Table 6.1.9-1: Oauth2 scopes defined in Nadm\_DM API**

Scope	Description
"nadm-dm"	Access to the Nadm_DM API
"nadm-dm:aiot-device-profile-data:read"	Access to read AIoT Device Profile Data
"nadm-dm:aiot-device-profile-data:modify"	Access to update AIoT Device Profile Data
"nadm-dm:af-authorization-data:read"	Access to read AF Authorization Data

## 6.1.10 HTTP redirection

An HTTP request may be redirected to a different ADM service instance when using direct or indirect communications (see 3GPP TS 29.500 [4]).

An SCP that reselects a different ADM producer instance will return the NF Instance ID of the new ADM producer instance in the 3gpp-Sbi-Producer-Id header, as specified in clause 6.10.3.4 of 3GPP TS 29.500 [4].

If an ADM redirects a service request to a different ADM using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new ADM towards which the service request is redirected shall be indicated in the 3gpp-Sbi-Target-Nf-Id header of the 307 Temporary Redirect or 308 Permanent Redirect response as specified in clause 6.10.9.1 of 3GPP TS 29.500 [4].

---

# Annex A (normative): OpenAPI specification

## A.1 General

This Annex specifies the formal definition of the API(s) defined in the present specification. It consists of OpenAPI specifications in YAML format.

This Annex takes precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API(s).

NOTE 1: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification files contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5.3.1 of 3GPP TS 29.501 [5] and clause 5B of 3GPP TR 21.900 [7]).

---

## A.2 Nadm\_DM API

```
openapi: 3.0.0

info:
  version: '1.0.0-alpha.4'
  title: 'Nadm_DM'
  description: |
    Nadm Data Management Service.
    © 2025, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.369 Ambient IoT Data Management Services, version 19.0.0
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.369/'

servers:
  - url: '{apiRoot}/nadm-dm/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501.

security:
  - oAuth2ClientCredentials:
    - nadm-dm
  - {}

paths:
  /aiot-device-profile-data/{aiotDevPermId}:
    get:
      summary: get AIoT Device Profile Data
      operationId: Get AIoT Device Profile Data
      tags:
        - AIoT Device Profile Data Retrieval
      parameters:
        - name: aiotDevPermId
          in: path
          description: AIoT Device Permanent ID
          required: true
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
      responses:
        '200':
          description: Expected response to a valid request
          content:
            application/json:
              schema:
```

```

    $ref: '#/components/schemas/AiotDevProfileData'
  '400':
    $ref: 'TS29571_CommonData.yaml#/components/responses/400'
  '401':
    $ref: 'TS29571_CommonData.yaml#/components/responses/401'
  '403':
    $ref: 'TS29571_CommonData.yaml#/components/responses/403'
  '404':
    description: Not Found
    content:
      application/problem+json:
        schema:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
  '406':
    $ref: 'TS29571_CommonData.yaml#/components/responses/406'
  '429':
    $ref: 'TS29571_CommonData.yaml#/components/responses/429'
  '500':
    $ref: 'TS29571_CommonData.yaml#/components/responses/500'
  '502':
    $ref: 'TS29571_CommonData.yaml#/components/responses/502'
  '503':
    $ref: 'TS29571_CommonData.yaml#/components/responses/503'
  default:
    description: Unexpected error
patch:
  summary: modify AIoT Device Profile Data
  operationId: Modify AIoT Device Profile Data
  tags:
    - AIoT Device Profile Data Update
  parameters:
    - name: aiotDevPermId
      in: path
      description: AIoT Device Permanent ID
      required: true
      schema:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
    - name: supported-features
      in: query
      description: Features required to be supported by the target NF
      schema:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
  requestBody:
    content:
      application/merge-patch+json:
        schema:
          $ref: '#/components/schemas/AiotDevProfileData'
    required: true
  responses:
    '204':
      description: Expected response to a valid request
    '200':
      description: Expected response to a valid request
      content:
        application/json:
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PatchResult'
    '400':
      $ref: 'TS29571_CommonData.yaml#/components/responses/400'
    '401':
      $ref: 'TS29571_CommonData.yaml#/components/responses/401'
    '403':
      $ref: 'TS29571_CommonData.yaml#/components/responses/403'
    '404':
      description: Not Found
      content:
        application/problem+json:
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
    '411':
      $ref: 'TS29571_CommonData.yaml#/components/responses/411'
    '413':
      $ref: 'TS29571_CommonData.yaml#/components/responses/413'
    '415':
      $ref: 'TS29571_CommonData.yaml#/components/responses/415'
    '429':
      $ref: 'TS29571_CommonData.yaml#/components/responses/429'
    '500':

```

```

    $ref: 'TS29571_CommonData.yaml#/components/responses/500'
  '502':
    $ref: 'TS29571_CommonData.yaml#/components/responses/502'
  '503':
    $ref: 'TS29571_CommonData.yaml#/components/responses/503'
  default:
    description: Unexpected error

```

```
/af-authorization-data:
```

```

  get:
    summary: get AF Authorization Data
    operationId: Get AF Authorization Data
    tags:
      - AF Authorization Data Retrieval
    parameters:
      - name: af-id
        in: query
        description: AF ID
        required: false
        schema:
          $ref: '#/components/schemas/AfId'
    responses:
      '200':
        description: Expected response to a valid request
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/AfAuthorizationData'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29571_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '404':
        description: Not Found
        content:
          application/problem+json:
            schema:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
      '406':
        $ref: 'TS29571_CommonData.yaml#/components/responses/406'
      '429':
        $ref: 'TS29571_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29571_CommonData.yaml#/components/responses/500'
      '502':
        $ref: 'TS29571_CommonData.yaml#/components/responses/502'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
    default:
      description: Unexpected error

```

```
components:
```

```

  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nadm-dm: Access to the Nadm_DM API
            nadm-dm:aiot-device-profile-data:read: Access to read AIoT Device Profile Data
            nadm-dm:aiot-device-profile-data:modify: Access to update AIoT Device Profile Data
            nadm-dm:af-authorization-data:read: Access to read AF Authorization Data

```

```
schemas:
```

```

#
# STRUCTURED TYPES
#

  AiotDevProfileData:
    description: Contains the AIoT Device Profile Data.
    type: object
    required:
      - aiotDevPermId
      - lastKnownAiotfInfo
    properties:

```

```
aiotDevPermId:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
lastKnownAiotfInfo:
  $ref: '#/components/schemas/LastKnownAiotfInfo'
```

```
LastKnownAiotfInfo:
  description: Contains the Last Known AIoTF Info.
  type: object
  required:
    - lastKnownAiotfInfoInd
  properties:
    lastKnownAiotfInfoInd:
      type: boolean
    lastKnownAiotfId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
    lastKnownAiotfAddress:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/IpAddr'
    lastKnownAiotfFqdn:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Fqdn'
```

```
IndividualAfAuthorizationData:
  description: Contains the AF Authorization Data for an invidual AF.
  type: object
  required:
    - afId
  properties:
    afId:
      $ref: '#/components/schemas/AfId'
    allowedArea:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotArea'
    allowedServiceOperations:
      type: array
      items:
        $ref: '#/components/schemas/AllowedServiceOperation'
    allowedTargetAiotDevices:
      type: array
      items:
        $ref: '#/components/schemas/AllowedTargetAiotDevice'
```

```
AllowedTargetAiotDevice:
  description: Contains the permanent AIoT Device ID or the filtering information
  type: object
  properties:
    aiotDevPermId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
    filteringInfo:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotFilteringInformation'
```

```
AfAuthorizationData:
  description: Contains the AF Authorization Data.
  type: object
  required:
    - afAuthData
  properties:
    afAuthData:
      type: object
      description: >
        'Map carrying the AF Authorization Data.
        The key of the map is the AF ID of the corresponding Authorization Data'
    additionalProperties:
      $ref: '#/components/schemas/IndividualAfAuthorizationData'
    minProperties: 1
```

```
#
# SIMPLE TYPES
#
```

```
AfId:
  description: Indicates the identifier used to identify the AF.
  type: string
```

```
#
# ENUMS
#
```

```
AllowedServiceOperation:
  description: The Allowed Service Operation.
  anyOf:
    - type: string
```

```
enum:  
- INVENTORY  
- READ  
- WRITE  
- PERMANENT_DISABLE  
- type: string
```

## Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2025-04	CT4#128	C4-251315 C4-251316 C4-251317 C4-251318 C4-251460				TS skeleton Implementation of pCRs agreed at CT4#128.	0.1.0
2025-05	CT4#129	C4-252212 C4-252270 C4-252335 C4-252339 C4-252436 C4-252337 C4-252365				TS skeleton Implementation of pCRs agreed at CT4#129.	0.2.0
2025-08	CT4#130	C4-253305 C4-253406 C4-253407 C4-253408 C4-253409 C4-253410 C4-253411				TS skeleton Implementation of pCRs agreed at CT4#130.	0.3.0
2025-09	CT#109	CP-252182				Presented for information and approval	1.0.0
2025-09	CT#109					Approved in TSG CT#109	19.0.0

---

# History

<b>Document history</b>		
V19.0.0	January 2026	Publication