

ETSI TS 129 369 V19.2.0 (2026-03)



TECHNICAL SPECIFICATION

**5G;
5G System; Ambient IoT Data Management Services;
Stage 3
(3GPP TS 29.369 version 19.2.0 Release 19)**



Reference

RTS/TSGC-0429369vj20

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.....	6
1 Scope	8
2 References	8
3 Definitions and abbreviations.....	9
3.1 Definitions	9
3.2 Abbreviations	9
4 Overview	9
5 Services offered by the ADM.....	9
5.1 Introduction	9
5.2 Nadm_DM Service.....	10
5.2.1 Service Description.....	10
5.2.2 Service Operations	10
5.2.2.1 Introduction.....	10
5.2.2.2 Query.....	10
5.2.2.2.1 General	10
5.2.2.2.2 AIoT Device Profile Data Retrieval	10
5.2.2.2.3 AF Authorization Data Retrieval.....	11
5.2.2.2.4 Bundled AIoT Device Profile Data Retrieval.....	11
5.2.3 Update	12
5.2.3.2 AIoT Device Profile Data Update	12
5.2.3.3 Bundled AIoT Device Profile Data Update.....	12
5.3 Nadm_Sec Service	13
5.3.1 Service Description.....	13
5.3.2 Service Operations	13
5.3.2.1 Introduction.....	13
5.3.2.2 RAND_Get.....	13
5.3.2.2.1 General	13
5.3.2.2.2 RAND Retrieval	14
5.3.2.3 Authentication_Get	14
5.3.2.3.1 General	14
5.3.2.3.2 Authentication Data Retrieval	14
5.3.2.4 SessionKey_Get	15
5.3.2.4.1 General	15
5.3.2.5 TID_Get	15
5.3.2.5.1 General	15
5.3.2.5.2 TID Retrieval.....	15
6 API Definitions	16
6.1 Nadm_DM Service API	16
6.1.1 Introduction.....	16
6.1.2 Usage of HTTP	17
6.1.2.1 General	17
6.1.2.2 HTTP standard headers	17
6.1.2.2.1 General	17
6.1.2.2.2 Content type	17
6.1.2.3 HTTP custom headers	17
6.1.3 Resources.....	17
6.1.3.1 Overview.....	17
6.1.3.2 Resource: AiotDeviceProfileData	18
6.1.3.2.1 Description	18

6.1.3.2.2	Resource Definition	18
6.1.3.2.3	Resource Standard Methods	19
6.1.3.3	Resource: AfAuthorizationData	21
6.1.3.3.1	Description	21
6.1.3.3.2	Resource Definition	21
6.1.3.3.3	Resource Standard Methods	22
6.1.3.4	Resource: BundledAiotDeviceProfileData	23
6.1.3.4.1	Description	23
6.1.3.4.2	Resource Definition	23
6.1.3.4.3	Resource Standard Methods	23
6.1.4	Custom Operations without associated resources	26
6.1.5	Notifications	26
6.1.6	Data Model	26
6.1.6.1	General	26
6.1.6.2	Structured data types	27
6.1.6.2.1	Introduction	27
6.1.6.2.2	Type: AiotDevProfileData	28
6.1.6.2.3	Type: LastKnownAiotfInfo	28
6.1.6.2.4	Type: IndividualAfAuthorizationData	29
6.1.6.2.5	Type: AllowedTargetAiotDevice	29
6.1.6.2.6	Type: AfAuthorizationData	29
6.1.6.2.7	Type: <u>TidHandlingInformation</u>	30
6.1.6.3	Simple data types and enumerations	30
6.1.6.3.1	Introduction	30
6.1.6.3.2	Simple data types	30
6.1.6.3.3	Enumeration: AllowedServiceOperation	30
6.1.6.3.4	Enumeration: TidType	31
6.1.7	Error Handling	31
6.1.7.1	General	31
6.1.7.2	Protocol Errors	31
6.1.7.3	Application Errors	31
6.1.8	Feature negotiation	31
6.1.9	Security	31
6.1.10	HTTP redirection	32
6.2	Nadm_Sec Service API	32
6.2.1	Introduction	32
6.2.2	Usage of HTTP	32
6.2.2.1	General	32
6.2.2.2	HTTP standard headers	33
6.2.2.2.1	General	33
6.2.2.2.2	Content type	33
6.2.2.3	HTTP custom headers	33
6.2.3	Resources	33
6.2.3.1	Overview	33
6.2.4	Custom Operations without associated resources	33
6.2.4.1	Overview	33
6.2.4.2	Operation: getRand	34
6.2.4.2.1	Description	34
6.2.4.2.2	Operation Definition	34
6.2.4.3	Operation: getAuthentication	34
6.2.4.3.1	Description	34
6.2.4.3.2	Operation Definition	34
6.2.4.4	Operation: getSessionKey	35
6.2.4.4.1	Description	35
6.2.4.4.2	Operation Definition	35
6.2.4.5	Operation: getTid	35
6.2.4.5.1	Description	35
6.2.4.5.2	Operation Definition	35
6.2.5	Notifications	36
6.2.6	Data Model	36
6.2.6.1	General	36
6.2.6.2	Structured data types	36

6.2.6.2.1	Introduction	36
6.2.6.2.2	Type: GetAuthenticationRequest	37
6.2.6.2.3	Type: AuthData	37
6.2.6.2.4	Type: AuthDataSet	37
6.2.6.2.5	Type: GetAuthenticationResponse	37
6.2.6.2.6	Type: GetSessionKeyRequest	37
6.2.6.2.7	Type: GetSessionKeyResponse	38
6.2.6.2.8	Type: GetTidRequest	38
6.2.6.2.9	Type: GetTidResponse	38
6.2.6.2.10	Type: GetRandResponse	38
6.2.6.3	Simple data types and enumerations	38
6.2.6.3.1	Introduction	38
6.2.6.3.2	Simple data types	38
6.2.7	Error Handling	39
6.2.7.1	General	39
6.2.7.2	Protocol Errors	39
6.2.7.3	Application Errors	39
6.2.8	Feature negotiation	39
6.2.9	Security	39
6.2.10	HTTP redirection	40
Annex A (normative): OpenAPI specification		41
A.1	General	41
A.2	Nadm_DM API	41
A.3	Nadm_Sec API	47
Annex B (informative): Change history		53
History		54

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".
- [18] 3GPP TS 33.369: " Security aspects of Ambient Internet of Things (AIoT) services for isolated private networks".
- [19] 3GPP TS 29.503: "5G System; Unified Data Management Services; 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:

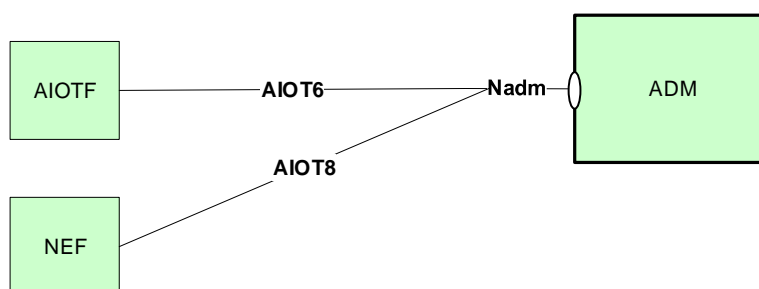


Figure 4-1: Reference model – ADM

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
- Nadm_Sec

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
Nadm_Sec	6.2	ADM Security Service	TS29369_Nadm_Sec.yaml	nadm-sec	A.3

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
- Bundled AIoT Device Profile 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 of a given AIoT device (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 of a given AIoT device.

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) sends a request to the ADM to receive the AF Authorization Data (see 3GPP TS 23.369 [14]).

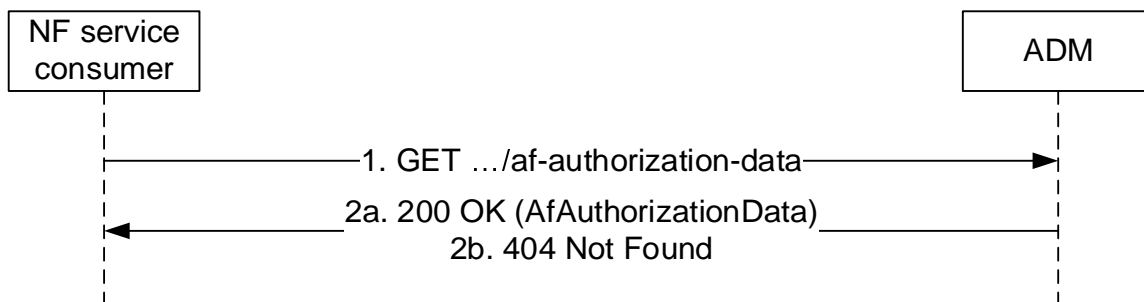


Figure 5.2.2.2.3-1: Requesting AF Authorization Data

1. The NF service consumer (e.g. AIOTF) 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.

5.2.2.2.4 Bundled AIoT Device Profile Data Retrieval

Figure 5.2.2.2.4-1 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 for bundled AIoT Devices (see 3GPP TS 23.369 [14]).

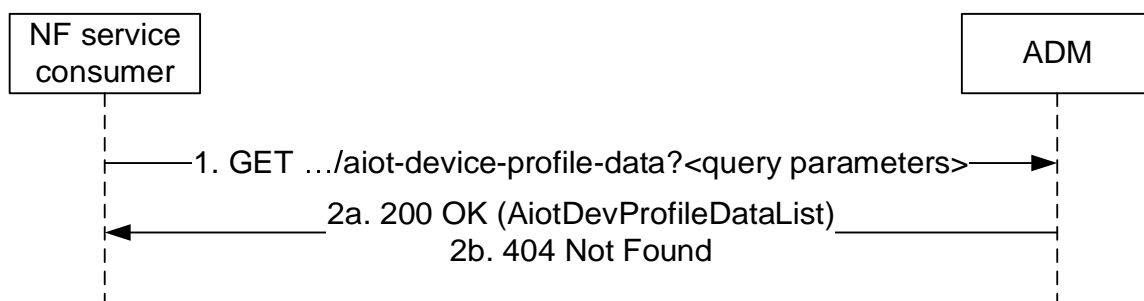


Figure 5.2.2.2.4-1: Requesting AIoT Device Profile Data for bundled AIoT Devices

1. The NF service consumer (e.g. AIOTF or NEF) sends a GET request to the resource URI "aiotDevPermId" collection resource. The optional input filter criteria (a list of aiotDevPermId) for the retrieval request may be included in the query parameters. All the aiotDevPermId included in the list are aggregated by the NF service consumer (e.g. AIOTF) based on the the list of device IDs served by ADM, which can be retrieved from NRF and included in the deviceIdList within AdmInfo.

The NF service consumer (e.g. AIOTF) should not include the `aiotDevPermId` that are not served by the ADM and after aggregation, the NF service consumer (e.g. AIOTF) shall bundle appropriate number of AIoT devices based on deployment to avoid bundling huge number of requested devices.

- 2a. On success, the ADM responds with "200 OK". The response body shall contain the URI (conforming to the resource URI structure as described in clause 5.2.2.2.2) of each `aiotDevPermId` in the ADM that satisfy the retrieval filter criteria (a list of `aiotDevPermId`).
- 2b. If there is no valid AIoT Device Profile Data for all the AIoT device permanent identifiers listed in the input filter criteria, 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

5.2.2.3.1 General

The following procedures using the Update service operation are supported:

- AIoT Device Profile Data Update
- Bundled AIoT Device Profile Data Update

5.2.2.3.2 AIoT Device Profile Data Update

Figure 5.2.2.3.2-1 shows a scenario where the NF service consumer (e.g., AIOTF) sends a request to the ADM to modify the AIoT Device Profile Data of a given AIoT device (see 3GPP TS 23.369 [14]). The request contains the AIoT device permanent identifier and the modification instructions.

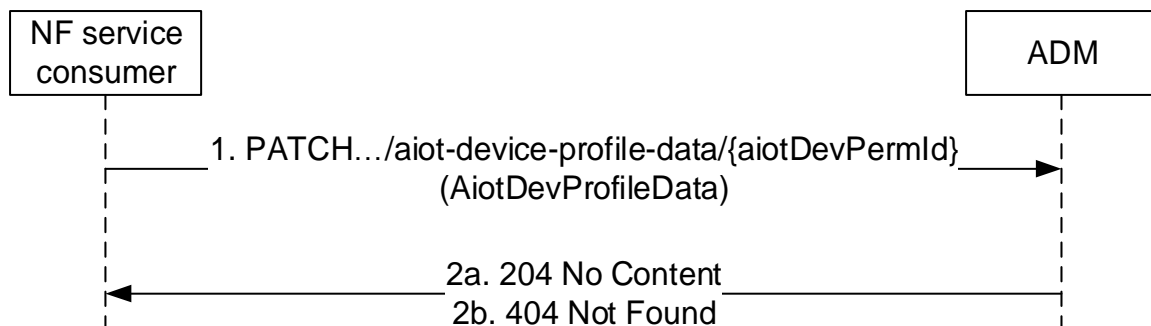


Figure 5.2.2.3.2-1: Updating AIoT Device Profile Data

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 of a given AIoT device.
- 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.

5.2.2.3.3 Bundled AIoT Device Profile Data Update

Figure 5.2.2.3.3-1 shows a scenario where the NF service consumer (e.g., AIOTF) sends a request to the ADM to modify the AIoT Device Profile Data for a bundled AIoT Devices (see 3GPP TS 23.369 [14]). The request contains the the modification instructions.

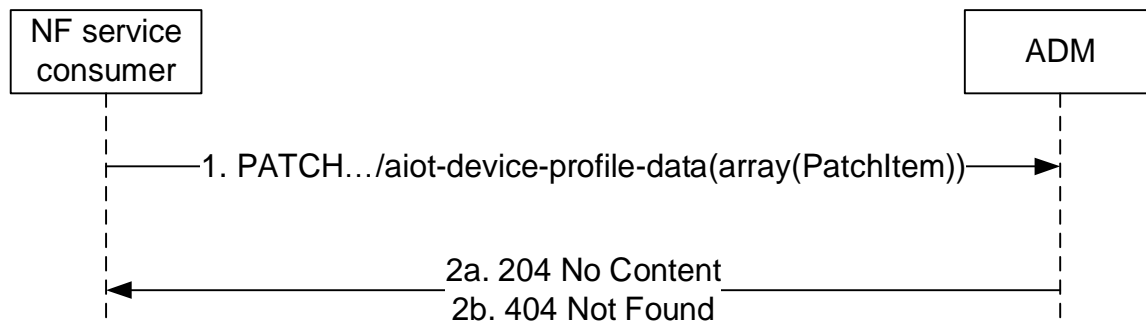


Figure 5.2.2.3.3-1: Updating AIoT Device Profile Data for bundled AIoT Devices

1. The NF service consumer (e.g. AIOTF) sends a PATCH request to the resource URI "aiotDevPermId" collection resource. The content of the PATCH request shall contain the list of operations (add/delete/replace) to be applied to the AIoT Device Profile Data for bundled AIoT Devices, these operations may be directed to bundled AIoT Devices, where each of them directed to individual AIoT Device Profile Data parameters for a given AIoT device permanent identifier or to all parameters offered by a given AIoT Device permanent identifier.
- 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.

5.3 Nadm_Sec Service

5.3.1 Service Description

See 3GPP TS 33.369 [18].

5.3.2 Service Operations

5.3.2.1 Introduction

For the Nadm_Sec service the following service operations are defined:

- RAND_Get
- Authentication_Get
- SessionKey_Get
- TID_Get

The Nadm_Sec Service is used by the AIOTF to request the ADM to provide a random number (RAND), authentication data for a single AIoT device or a group of AIoT devices, the session key for an AIoT device, and the T-ID for an AIoT device.

5.3.2.2 RAND_Get

5.3.2.2.1 General

The following procedures using the RAND_Get service operation are supported:

- RAND Retrieval

5.3.2.2.2 RAND Retrieval

Figure 5.3.2.2.2-1 shows a scenario where the NF service consumer (e.g. AIOTF) sends a request to the ADM to receive a random number (see 3GPP TS 33.369 [18]).

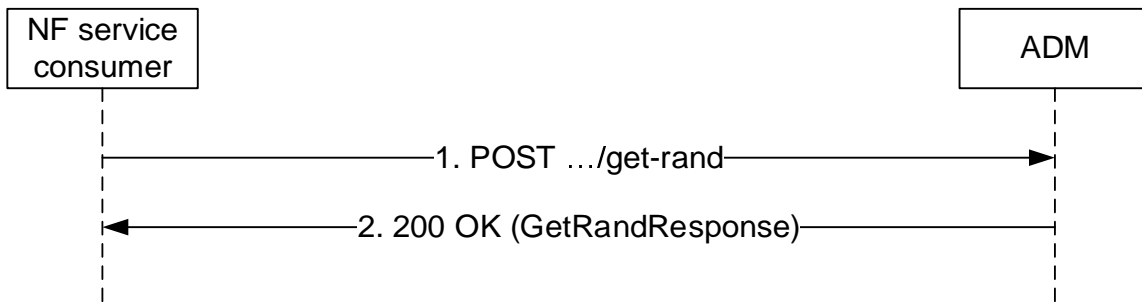


Figure 5.3.2.2.2-1: RAND Retrieval

1. The NF service consumer sends a POST request (custom method: get-rand).
2. The ADM responds with "200 OK" with the message body containing the generated random number.

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

5.3.2.3 Authentication_Get

5.3.2.3.1 General

The following procedures using the Authentication_Get service operation are supported:

- Authentication Data Retrieval

5.3.2.3.2 Authentication Data Retrieval

Figure 5.3.2.3.2-1 shows a scenario where the NF service consumer (e.g. AIOTF) sends a request to the ADM to receive the authentication data for a single AIoT device or a group of AIoT devices (see 3GPP TS 33.369 [18]).

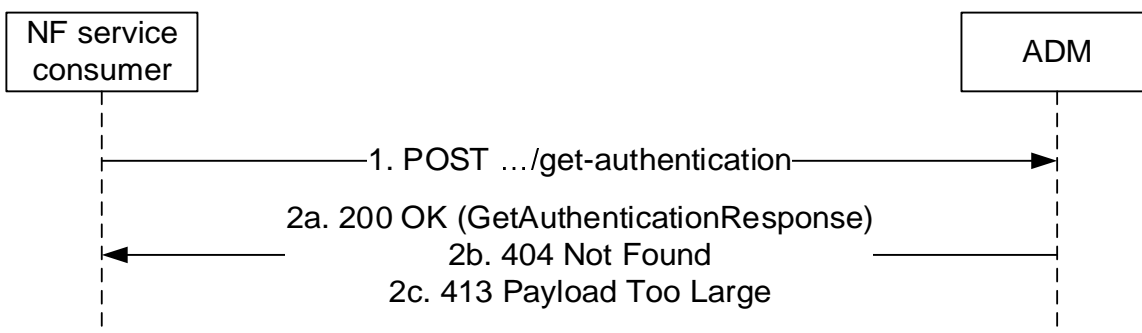


Figure 5.3.2.3.2-1: Authentication Data Retrieval

1. The NF service consumer sends a POST request (custom method: get-authentication) to the ADM, including authentication input parameters for a single AIoT Device, identified by an AIoT device permanent identifier, or a group of AIoT Devices, identified by Filter Information.
- 2a. The ADM responds with "200 OK" with the message body containing the derived authentication data.

2b. If the AIoT device permanent identifier or Filtering Information is not recognized, HTTP status code "404 Not Found" may be returned including additional error information in the response body (in the "ProblemDetails" element).

2c. If the group of devices derived from the Filtering Information is too large to compute the expected authentication data (XRES_{AIOT} values) in a reasonable amount of time, HTTP status code "413 Payload Too Large" may be returned. The ADM shall include the application error "FILTER_INFORMATION_TOO_BROAD" in the ProblemDetails element to indicate that the filtering criteria resulted in an unmanageable device set.

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

5.3.2.4 SessionKey_Get

5.3.2.4.1 General

The following procedures using the SessionKey_Get service operation are supported:

- Session Key Retrieval

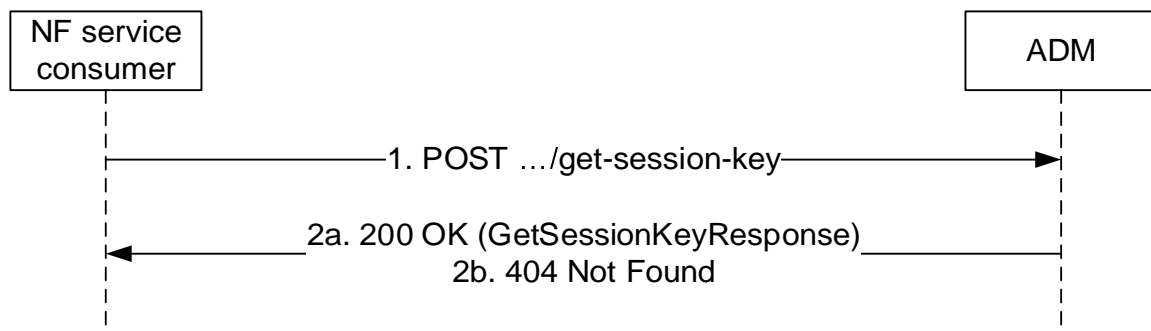


Figure 5.3.2.4.2-1: Session Key Retrieval

1. The NF service consumer sends a POST request (custom method: get-session-key) to the ADM, including input parameters for an AIoT Device, identified by an AIoT device permanent identifier.
- 2a. The ADM responds with "200 OK", with the message body containing the derived Session Key.
- 2b. If the AIoT device permanent identifier is not recognized, HTTP status code "404 Not Found" may 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 POST response body.

5.3.2.5 TID_Get

5.3.2.5.1 General

The following procedures using the TID_Get service operation are supported:

- TID Retrieval

5.3.2.5.2 TID Retrieval

Figure 5.3.2.5.2-1 shows a scenario where the NF service consumer (e.g. AIOTF) sends a request to the ADM to receive the TID (see 3GPP TS 33.369 [18]).

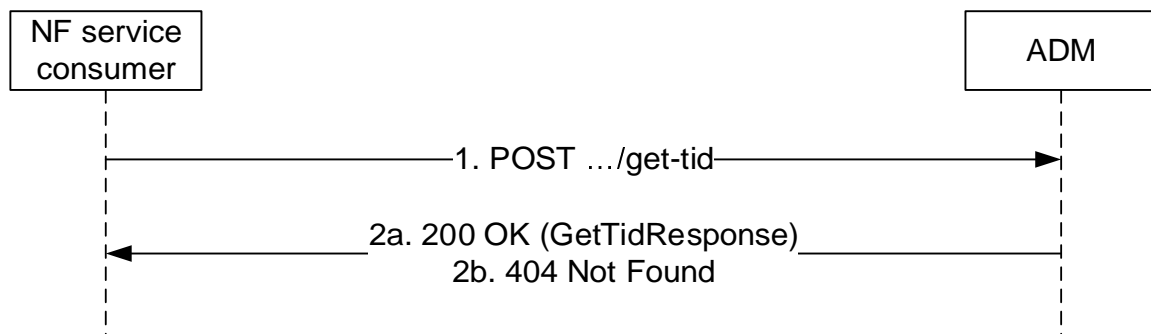


Figure 5.3.2.5.2-1: TID Retrieval

1. The NF service consumer sends a POST request (custom method: get-tid) to the ADM, including input parameters such as the AIoT device permanent identifier and, optionally, a resynchronization indicator.
- 2a. The ADM responds with "200 OK", with the message body containing the allocated Temporary ID (T-ID) and the associated T-ID handling information.
- 2b. If the AIoT device permanent identifier is not recognized, HTTP status code "404 Not Found" may 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 POST 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.

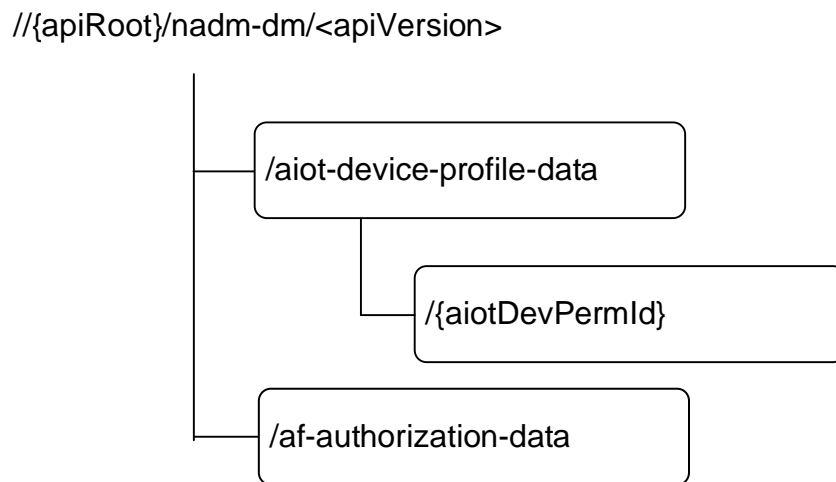


Figure 6.1.3.1-1: Resource URI structure of the Nadm_DM API

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/{aiotDevPermId}	GET	Retrieve AIoT Device Profile Data
		PATCH	Modify AIoT Device Profile Data
BundledAiotDeviceProfileData	/aiot-device-profile-data	GET	Retrieve AIoT Device Profile Data of bundled AIoT Devices.
		PATCH	Modify AIoT Device Profile Data of bundled AIoT Devices.
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
aiotDevPermlId	AiotDevPermlId	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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (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: 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.

NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].

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

Table 6.1.3.2.3.1-6: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.2.3.1-7: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected.

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 3)
PatchResult	M	1	200 OK	Upon success, the execution report is returned. (NOTE 2)
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (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: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. NOTE 3: 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.				

Table 6.1.3.2.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.2.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected.

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.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (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: 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.				
NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

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 6.1.3.3.3.1-5: 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

Table 6.1.3.3.3.1-6: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.3.3.1-7: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected.

6.1.3.4 Resource: BundledAiotDeviceProfileData

6.1.3.4.1 Description

This resource is used to represent a collection resource of different AiotDeviceProfileData with the resource URI "aiotDevPermId".

6.1.3.4.2 Resource Definition

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

This resource shall support the resource URI variables defined in table 6.1.3.4.2-1.

Table 6.1.3.4.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.1.1

6.1.3.4.3 Resource Standard Methods

6.1.3.4.3.1 GET

This method shall support the URI query parameters specified in table 6.1.3.4.3.1-1.

Table 6.1.3.4.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description	Applicability
requester-aiot-devices-id	array(AiotDevP ermId)	M	1..N	This IE shall contain a list of the requested AIoT device permanent identifier.	

This method shall support the request data structures specified in table 6.1.3.4.3.1-2 and the response data structures and response codes specified in table 6.1.3.4.3.1-3.

Table 6.1.3.4.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.1.3.4.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AiotDevProfileDataList	M	1	200 OK	Upon success, a response body containing the AIoT Device Profile Data for bundled AIoT Devices shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (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: 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.

NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].

Table 6.1.3.4.3.1-4: 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 6.1.3.4.3.1-5: 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

Table 6.1.3.4.3.1-6: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.4.3.1-7: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected.

6.1.3.4.3.2 PATCH

This method shall support the URI query parameters specified in table 6.1.3.4.3.2-1.

Table 6.1.3.4.3.2-1: 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 6.1.3.4.3.2-2 and the response data structures and response codes specified in table 6.1.3.4.3.2-3.

Table 6.1.3.4.3.2-2: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
array(PatchItem)	M	1..N	It contains the list of changes to be made to the AIoT Device Profile Data for bundled AIoT Devices, according to the JSON PATCH format specified in IETF RFC 6902 [13].

Table 6.1.3.4.3.2-3: 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 3)
PatchResult	M	1	200 OK	Upon success, the execution report is returned. (NOTE 2)
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (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: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. NOTE 3: 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.				

Table 6.1.3.4.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.4.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the Callback URI of the target NF Service Consumer (e.g. ADM) to which the request is redirected. For the case, when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected.

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	
TidHandlingInformation	6.1.6.2.7	T-ID handling information	
AiotDevProfileDataList	6.1.6.2.8	AIoT Device Profile Data of bundled AIoT Devices	
LastKnownAiotfInfoInd	6.1.6.3.2	Last known AIoTF Information	
Afid	6.1.6.3.2	AF ID	
Tid	6.1.6.3.2	Temporary ID (T-ID) of the AIoT device	
AllowedServiceOperation	6.1.6.3.3	Allowed Service Operation	
TidType	6.1.6.3.4	Represent T-ID Type	

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
AiotDevPermlId	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
aiotDevPermlId	AiotDevPermlId	M	1	Globally unique AIoT device permanent identifier	
lastKnownAiotfInfo	LastKnownAiotfInfo	M	1	Indicate the last known AIOTF that serves the AIoT device, or unknown.	
tidCurrent	Tid	O	0..1	Current Temporary Identifier (T-ID_n) as specified in 3GPP TS 33.369 [18].	
tidPrevious	Tid	O	0..1	Previous Temporary Identifier (T-ID_n-1) as specified in 3GPP TS 33.369 [18].	
tidHandlingInformation	TidHandlingInformation	O	0..1	T-ID handling information as specified in clause 5.4.3 of 3GPP TS 33.369 [18].	

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	O	0..1	This IE may be present when lastKnownAiotfInfoInd is set to true. Indicates the last known AIOTF instance (NOTE)	
lastKnownAiotfAddress	IpAddr	O	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	O	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	O	0..1	If present, it indicates the allowed area for the indicated AF to perform the AIoT service operations. If this attribute is absent, it means that the complete service area is allowed for the AF.	
allowedServiceOperations	array(AllowedServiceOperation)	O	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)	O	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	C	0..1	Indicates the AIoT Device Permanent ID. (NOTE)	
filteringInfo	AiotFilteringInformation	C	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.	

6.1.6.2.7 Type: TidHandlingInformation**Table 6.1.6.2.7-1: Definition of type TidHandlingInformation**

Attribute name	Data type	P	Cardinality	Description	Applicability
tidType	TidType	M	1	Indicates the T-ID handling type.	
tidTypeUpdateInd	boolean	C	0..1	This IE shall be present if the TidType set to "STORED". Indicates whether the stored T-ID is updated with a command via a Command procedure or without a command. true: indicates that the stored T-ID is updated with a command via a Command procedure. false: indicates that the stored T-ID is updated without a command.	

6.1.6.2.8 Type: AiotDevProfileDataList

Table 6.1.6.2.8-1: Definition of type AiotDevProfileDataList

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevProfileDataList	array(AiotDevProfileData)	M	1..N	This IE indicates the AIoT Device Profile Data of a list of AIoT devices.	

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.	
Tid	string	pattern: "[A-Fa-f0-9]{32}\$"	

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.	

6.1.6.3.4 Enumeration: TidType

Table 6.3.6.3.4-1: Enumeration TidType

Enumeration value	Description
"STORED"	Indicates the stored type of T-ID
"CONCEALED"	Indicates the concealed type of T-ID

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].

6.2 Nadm_Sec Service API

6.2.1 Introduction

The Nadm_Sec shall use the Nadm_Sec API.

The API URI of the Nadm_Sec 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-sec".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.2.3.

6.2.2 Usage of HTTP

6.2.2.1 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_Sec API is contained in Annex A.

6.2.2.2 HTTP standard headers

6.2.2.2.1 General

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

6.2.2.2.2 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].

6.2.2.3 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.

6.2.3 Resources

6.2.3.1 Overview

There are no resources defined for this API in this release of the specification.

6.2.4 Custom Operations without associated resources

6.2.4.1 Overview

This clause describes the structure for custom operations without associated resources.

Figure 6.2.4.1-1 depicts the custom operation URIs structure for the Nadm_Sec API.

//{apiRoot}/nadm-sec/<apiVersion>

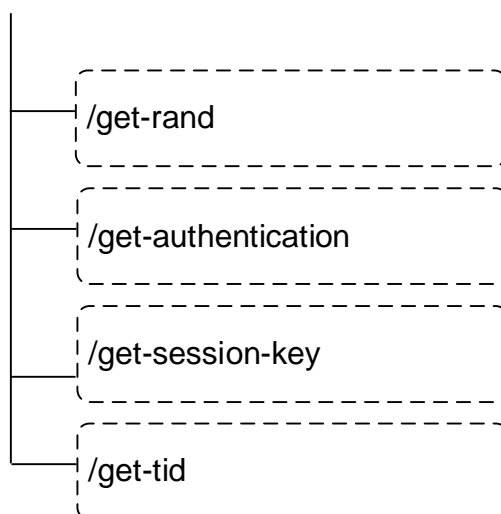


Figure 6.2.4.1-1: Custom operation URI structure of the Nadm_Sec API

Table 6.2.4.1-1 provides an overview of the custom operations and applicable HTTP methods.

Table 6.2.4.1-1: Custom operations without associated resources

Resource purpose/name	Resource URI (relative path after API URI)	HTTP method or custom operation	Description (service operation)
getRand	/get-rand	POST	Retrieve a random number from ADM
getAuthentication	/get-authentication	POST	Retrieve authentication data from ADM
getSessionKey	/get-session-key	POST	Retrieve a session key from ADM
getTid	/get-tid	POST	Retrieve a T-ID from ADM

6.2.4.2 Operation: getRand

6.2.4.2.1 Description

The custom operation enables to generate and retrieve a random number. See 3GPP TS 33.369 [18].

6.2.4.2.2 Operation Definition

This operation shall support the request data structures specified in table 6.2.4.2.2-1 and the response data structure and response codes specified in table 6.2.4.2.2-2.

Table 6.2.4.2.2-1: Data structures supported by the POST Request Body on this custom operation

Data type	P	Cardinality	Description
n/a			

Table 6.2.4.2.2-2: Data structures supported by the POST Response Body on this custom operation

Data type	P	Cardinality	Response codes	Description
GetRandResponse	M	1	200 OK	Upon success, a response body containing the generated random value $RAND_{AIOT_n}$ shall be returned
NOTE: In addition common data structures as listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] are supported.				

6.2.4.3 Operation: getAuthentication

6.2.4.3.1 Description

This custom operation enables to calculate and retrieve the authentication data. See 3GPP TS 33.369 [18].

6.2.4.3.2 Operation Definition

This operation shall support the request data structures specified in table 6.2.4.3.2-1 and the response data structure and response codes specified in table 6.2.4.3.2-2.

Table 6.2.4.3.2-1: Data structures supported by the POST Request Body on this custom operation

Data type	P	Cardinality	Description
GetAuthenticationRequest	M	1	Contains input parameters required to retrieve authentication data from ADM.

Table 6.2.4.3.2-2: Data structures supported by the POST Response Body on this custom operation

Data type	P	Cardinality	Response codes	Description
GetAuthenticationResponse	M	1	200 OK	Upon success, a response body containing the authentication data shall be returned
NOTE: In addition common data structures as listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] are supported.				

6.2.4.4 Operation: getSessionKey

6.2.4.4.1 Description

This custom operation enables to calculate and retrieve the Session Key. See 3GPP TS 33.369 [18].

6.2.4.4.2 Operation Definition

This operation shall support the request data structures specified in table 6.2.4.4.2-1 and the response data structure and response codes specified in table 6.2.4.4.2-2.

Table 6.2.4.4.2-1: Data structures supported by the POST Request Body on this custom operation

Data type	P	Cardinality	Description
GetSessionKeyRequest	M	1	Contains input parameters required to retrieve the Session Key from ADM.

Table 6.2.4.4.2-2: Data structures supported by the POST Response Body on this custom operation

Data type	P	Cardinality	Response codes	Description
GetSessionKeyResponse	M	1	200 OK	Upon success, a response body containing the Session Key shall be returned
NOTE: In addition common data structures as listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] are supported.				

6.2.4.5 Operation: getTid

6.2.4.5.1 Description

This custom operation enables to derive a T-ID. See 3GPP TS 33.369 [18].

6.2.4.5.2 Operation Definition

This operation shall support the request data structures specified in table 6.2.4.5.2-1 and the response data structure and response codes specified in table 6.2.4.5.2-2.

Table 6.2.4.5.2-1: Data structures supported by the POST Request Body on this custom operation

Data type	P	Cardinality	Description
GetTidRequest	M	1	Contains input parameters for retrieving the T-ID.

Table 6.2.4.5.2-2: Data structures supported by the POST Response Body on this custom operation

Data type	P	Cardinality	Response codes	Description
GetTidResponse	M	1	200 OK	Upon success, a response body containing the T-ID information shall be returned
NOTE: In addition common data structures as listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] are supported.				

6.2.5 Notifications

6.2.6 Data Model

6.2.6.1 General

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

Table 6.2.6.1-1 specifies the data types defined for the Nadm_Sec service based interface protocol.

Table 6.2.6.1-1: Nadm_Sec specific Data Types

Data type	Clause defined	Description	Applicability
GetAuthenticationRequest	6.2.6.2.2	Contains input parameters for computing authentication data	
AuthData	6.2.6.2.3	Authentication Data	
AuthDataSet	6.2.6.2.4	Authentication Data Set	
GetAuthenticationResponse	6.2.6.2.5	Contains authentication data	
GetSessionKeyRequest	6.2.6.2.6	Contains input parameters for computing a session key	
GetSessionKeyResponse	6.2.6.2.7	Contains a session key information	
GetTidRequest	6.2.6.2.8	Contains input parameters for retrieving the T-ID	
GetTidResponse	6.2.6.2.9	Contains T-ID information	
GetRandResponse	6.2.6.2.10	Contains RAND information	
Kaiotf	6.2.6.3.2	AIoT session key K_{AIOTF}	

Table 6.2.6.1-2 specifies data types re-used by the Nadm_Sec 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_Sec service based interface.

Table 6.2.6.1-2: Nadm_Sec 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
AiotDevPerMld	3GPP TS 29.571 [17]	AIoT device permanent identifier	
AiotFilteringInformation	3GPP TS 29.571 [17]	AIoT Filtering Information	
ProblemDetails	3GPP TS 29.571 [17]	Used in error responses to provide more detailed information about an error.	
Tid	6.1.6.3.2	Temporary ID (T-ID) of the AIoT device	
TidHandlingInformation	6.1.6.2.7	T-ID Handling Information	
Rand	3GPP TS 29.503 [19]	RAND	
Xres	3GPP TS 29.503 [19]	XRES	

6.2.6.2 Structured data types

6.2.6.2.1 Introduction

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

6.2.6.2.2 Type: GetAuthenticationRequest

Table 6.2.6.2.2-1: Definition of type GetAuthenticationRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevPermId	AiotDevPermId	O	0..1	Indicates the AIoT device permanent identifier.	
filteringInfo	AiotFilteringInformation	O	0..1	Indicates the AIoT Filtering Information.	
randN	Rand	M	1	Indicates the RAND _{AIOT_n} .	
randDlist	array(Rand)	M	1..N	Indicates the RAND _{AIOT_d} (s).	

6.2.6.2.3 Type: AuthData

Table 6.2.6.2.3-1: Definition of type AuthData

Attribute name	Data type	P	Cardinality	Description	Applicability
xres	Xres	M	1	Contains the calculated XRES.	
aiotDevPermId	AiotDevPermId	C	0..1	This attribute shall be present if the aiotDevPermId attribute is not provided in the GetAuthenticationRequest data type. Indicates the AIoT device permanent identifier used to calculate the XRES.	

6.2.6.2.4 Type: AuthDataSet

Table 6.2.6.2.4-1: Definition of type AuthDataSet

Attribute name	Data type	P	Cardinality	Description	Applicability
randD	Rand	M	1	Indicates the RAND _{AIOT_d} used to derive the authentication data	
authDataSet	array(AuthData)	M	1..N	Contains the list of calculated XRES.	

6.2.6.2.5 Type: GetAuthenticationResponse

Table 6.2.6.2.5-1: Definition of type GetAuthenticationResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
authDataSets	array(AuthDataSet)	M	1..N	Indicates the list of Authentication Data Set	

6.2.6.2.6 Type: GetSessionKeyRequest

Table 6.2.6.2.6-1: Definition of type GetSessionKeyRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevPermId	AiotDevPermId	M	1	Indicates an AIoT device permanent identifier. (NOTE)	
randN	Rand	M	1	Indicates the RAND _{AIOT_n} .	
randD	Rand	M	1	Indicates the RAND _{AIOT_d} .	

6.2.6.2.7 Type: GetSessionKeyResponse

Table 6.2.6.2.7-1: Definition of type GetSessionKeyResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
kAioTf	Kaiotf	M	1	Contains the Session Key	

6.2.6.2.8 Type: GetTidRequest

Table 6.2.6.2.8-1: Definition of type GetTidRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
aiotDevPerMId	AiotDevPerMId	M	1	Indicates an AIoT device permanent identifier.	
resyncInd	boolean	O	0..1	Indicates if re-synchronization is required. true: re-synchronization is required; false (or absent): re-synchronization is not required;	

6.2.6.2.9 Type: GetTidResponse

Table 6.2.6.2.9-1: Definition of type GetTidResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
tidHandInfo	TidHandlingInformation	M	1	Indicate T-ID Handling Information	
tid	Tid	M	1	Current Temporary Identifier (T-ID _n) as specified in 3GPP TS 33.369 [18]	
tidPrevious	Tid	O	0..1	Previous Temporary Identifier (T-ID _{n-1}) as specified in 3GPP TS 33.369 [18].	

6.2.6.2.10 Type: GetRandResponse

Table 6.2.6.2.10-1: Definition of type GetRandResponse

Attribute name	Data type	P	Cardinality	Description	Applicability
randN	Rand	M	1	Indicates the RAND _{AIOT_n}	

6.2.6.3 Simple data types and enumerations

6.2.6.3.1 Introduction

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

6.2.6.3.2 Simple data types

The simple data types defined in table 6.2.6.3.2-1 shall be supported.

Table 6.2.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
Kaiotf	string	pattern: "[A-Fa-f0-9]{32}\$"	

6.2.7 Error Handling

6.2.7.1 General

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

6.2.7.2 Protocol Errors

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

6.2.7.3 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_Sec. The application errors defined for the Nadm_Sec service are listed in Table 6.2.7.3-1.

Table 6.2.7.3-1: Application errors

Application Error	HTTP status code	Description
DATA_NOT_FOUND	404 Not Found	The AIoT device permanent identifier or Filtering Information is not recognized.
FILTER_INFORMATION_TOO_BROAD	413 Payload Too Large	The group of devices derived from the Filtering Information is too large to compute the expected authentication data in a reasonable amount of time.

6.2.8 Feature negotiation

The optional features in table 6.2.8-1 are defined for the Nadm_Sec API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.2.8-1: Supported Features

Feature number	Feature Name	Description

6.2.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Nadm_Sec 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 Nadm_Sec 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 Nadm_Sec service.

The Nadm_Sec API defines the following scopes for OAuth2 authorization.

Table 6.2.9-1: OAuth2 scopes defined in Nadm_Sec API

Scope	Description
"nadm-sec"	Access to the Nadm_Sec API
"nadm-sec:get-rand:invoke "	Access to retrieve a RAND
"nadm-sec:get-authentication:invoke "	Access to retrieve Authentication Data
"nadm-sec:get-session-key:invoke "	Access to retrieve a Session Key
"nadm-sec:get-tid:invoke "	Access to retrieve a T-ID

6.2.10 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: '1.0.1'
  title: 'Nadm_DM'
  description: |
    Nadm Data Management Service.
    © 2026, 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 19.2.0
  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 for a give AIoT Device
      operationId: Get AIoT Device Profile Data
      tags:
        - AIoT Device Profile Data Retrieval
      security:
        - {}
        - oAuth2ClientCredentials:
          - nadm-dm
        - oAuth2ClientCredentials:
          - nadm-dm
          - nadm-dm:aiot-device-profile-data:read
      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'
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29571_CommonData.yaml#/components/responses/308'
    '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 for a give AIoT Device
  operationId: Modify AIoT Device Profile Data
  tags:
    - AIoT Device Profile Data Update
  security:
    - {}
    - oAuth2ClientCredentials:
        - nadm-dm
    - oAuth2ClientCredentials:
        - nadm-dm
        - nadm-dm:aiot-device-profile-data:modify
  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:
    '200':
      description: Expected response to a valid request
      content:
        application/json:
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PatchResult'
    '204':
      description: Expected response to a valid request
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':

```

```

    $ref: 'TS29571_CommonData.yaml#/components/responses/308'
  '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

```

/aiot-device-profile-data:

```

get:
  summary: get AIoT Device Profile Data for a bundled AIoT Devices
  operationId: Get Bundled AIoT Device Profile Data
  tags:
    - Bundled AIoT Device Profile Data Retrieval
  security:
    - {}
    - oAuth2ClientCredentials:
        - nadm-dm
    - oAuth2ClientCredentials:
        - nadm-dm
        - nadm-dm:aiot-device-profile-data:read
  parameters:
    - name: requester-aiot-devices-id
      in: query
      description: a list of AIoT Device Permanent ID
      required: true
      style: form
      explode: false
      schema:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
        minItems: 1
  responses:
    '200':
      description: Expected response to a valid request
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/AiotDevProfileDataList'
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29571_CommonData.yaml#/components/responses/308'
    '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':
      $ref: 'TS29571_CommonData.yaml#/components/responses/404'
    '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 bundled AIoT Device Profile Data for bundled AIoT devices.
  operationId: Modify bundled AIoT Device Profile Data
  tags:
    - Bundled AIoT Device Profile Data Update
  security:
    - {}
    - oAuth2ClientCredentials:
      - nadm-dm
    - oAuth2ClientCredentials:
      - nadm-dm
      - nadm-dm:aiot-device-profile-data:modify
  parameters:
    - 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:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PatchItem'
    required: true
  responses:
    '200':
      description: Expected response to a valid request
      content:
        application/json:
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PatchResult'
    '204':
      description: Expected response to a valid request
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29571_CommonData.yaml#/components/responses/308'
    '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':
      $ref: 'TS29571_CommonData.yaml#/components/responses/404'
    '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
security:
  - {}
  - oAuth2ClientCredentials:
    - nadm-dm
  - oAuth2ClientCredentials:
    - nadm-dm
    - nadm-dm:af-authorization-data:read
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'
  '307':
    $ref: 'TS29571_CommonData.yaml#/components/responses/307'
  '308':
    $ref: 'TS29571_CommonData.yaml#/components/responses/308'
  '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'
tidCurrent:
  $ref: '#/components/schemas/Tid'
tidPrevious:
  $ref: '#/components/schemas/Tid'
tidHandlingInformation:
  $ref: '#/components/schemas/TidHandlingInformation'

```

```

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 individual 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'
    minItems: 1
  allowedTargetAiotDevices:
    type: array
    items:
      $ref: '#/components/schemas/AllowedTargetAiotDevice'
    minItems: 1

```

```

AllowedTargetAiotDevice:
description: >
  Contains the permanent AIoT Device ID or the filtering information,
  either aiotDevPermId, or filteringInfo shall be present.
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

```

```

Tid:
  description: Temporary ID of the AIoT device.
  type: string
  pattern: '^[A-Fa-f0-9]{32}$'

TidHandlingInformation:
  description: Contains the T-ID handling information
  type: object
  required:
    - tidType
  properties:
    tidType:
      $ref: '#/components/schemas/TidType'
    tidHandlingInformation:
      type: boolean

AiotDevProfileDataList:
  description: AIoT Device Profile Data of a list of AIoT devices.
  type: object
  required:
    - aiotDevProfileDataList
  properties:
    aiotDevProfileDataList:
      type: array
      items:
        $ref: '#/components/schemas/AiotDevProfileData'
      minItems: 1

#
# ENUMS
#

AllowedServiceOperation:
  description: The Allowed Service Operation.
  anyOf:
    - type: string
      enum:
        - INVENTORY
        - READ
        - WRITE
        - PERMANENT_DISABLE
    - type: string

TidType:
  description: Indicates the type of T-ID.
  anyOf:
    - type: string
      enum:
        - STORED
        - CONCEALED
    - type: string

```

A.3 Nadm_Sec API

openapi: 3.0.0

```

info:
  version: '1.0.1'
  title: 'Nadm_Sec'
  description: |
    Nadm_Sec Service.
    © 2026, 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 19.2.0
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.369/'

```

```

servers:
  - url: '{apiRoot}/nadm-sec/v1'
    variables:
      apiRoot:

```

```
default: https://example.com
description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501.
```

```
security:
- oauth2ClientCredentials:
- nadm-sec
- {}

paths:
/get-rand:
post:
summary: Retrieve a random value (RANDAIOT_n)
operationId: getRand
tags:
- Get Rand
security:
- {}
- oAuth2ClientCredentials:
- nadm-sec
- oAuth2ClientCredentials:
- nadm-sec
- nadm-sec:get-rand:invoke
responses:
'200':
description: Successful retrieval of RANDAIOT_n
content:
application/json:
schema:
$ref: '#/components/schemas/GetRandResponse'
'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':
$ref: 'TS29571_CommonData.yaml#/components/responses/404'
'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
/get-authentication:
post:
summary: Retrieve authentication data (XRESAIOT)
operationId: getAuthentication
requestBody:
required: true
content:
application/json:
schema:
$ref: '#/components/schemas/GetAuthenticationRequest'
tags:
- Get Authentication
security:
- {}
- oAuth2ClientCredentials:
- nadm-sec
- oAuth2ClientCredentials:
- nadm-sec
- nadm-sec:get-authentication:invoke
responses:
'200':
description: Successful retrieval of authentication data
content:
application/json:
schema:
```

```

        $ref: '#/components/schemas/GetAuthenticationResponse'
'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':
  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
'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
/get-session-key:
  post:
    summary: Retrieve session key (KAIOTF)
    operationId: getSessionKey
    tags:
      - Get Session Key
    security:
      - {}
      - oAuth2ClientCredentials:
          - nadm-sec
      - oAuth2ClientCredentials:
          - nadm-sec
          - nadm-sec:get-session-key:invoke
    requestBody:
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/GetSessionKeyRequest'
    responses:
      '200':
        description: Successful retrieval of session key
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/GetSessionKeyResponse'
      '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':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '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
/get-tid:
  post:
    summary: Retrieve Temporary ID (T-ID)

```

```

    operationId: getTid
    tags:
      - Get Tid
    security:
      - {}
      - oAuth2ClientCredentials:
          - nadm-sec
      - oAuth2ClientCredentials:
          - nadm-sec
          - nadm-sec:get-tid:invoke
    requestBody:
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/GetTidRequest'
    responses:
      '200':
        description: Successful retrieval of T-ID
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/GetTidResponse'
      '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':
        $ref: 'TS29571_CommonData.yaml#/components/responses/404'
      '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
  components:
    securitySchemes:
      oAuth2ClientCredentials:
        type: oauth2
        flows:
          clientCredentials:
            tokenUrl: https://example.com/oauth2/token
            scopes:
              nadm-sec: Access to Nadm_Sec API
              nadm-sec:get-rand:invoke: Access to retrieve a RAND
              nadm-sec:get-authentication:invoke: Access to retrieve Authentication Data
              nadm-sec:get-session-key:invoke: Access to retrieve a Session Key
              nadm-sec:get-tid:invoke: Access to retrieve a T-ID
    schemas:
#
# STRUCTURED TYPES
#

  GetRandResponse:
    type: object
    description: Contains the RandN.
    properties:
      randN:
        $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
    required:
      - randN

  GetAuthenticationRequest:
    type: object
    description: Contains the Rand and AIoT identifications.
    properties:

```

```

    aiotDevPermId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
    filteringInfo:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotFilteringInformation'
    randN:
      $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
    randDlist:
      type: array
      items:
        $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
      minItems: 1
    required:
    - randN
    - randDlist

AuthData:
  type: object
  description: >
    Contains the calculated XRES and optionally the AIoT device permanent
    identifier used to calculate it.
  properties:
    xres:
      $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Xres'
    aiotDevPermId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
  required:
  - xres

AuthDataSet:
  type: object
  description: Contains a RANDAIOT_d value and a list of associated AuthData entries.
  properties:
    randD:
      $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
    authDataSet:
      type: array
      items:
        $ref: '#/components/schemas/AuthData'
      minItems: 1
  required:
  - randD
  - authDataSet

GetAuthenticationResponse:
  type: object
  description: Response type containing one or more AuthDataSet entries.
  properties:
    authDataSets:
      type: array
      items:
        $ref: '#/components/schemas/AuthDataSet'
      minItems: 1
  required:
  - authDataSets

GetSessionKeyRequest:
  type: object
  description: Contains a AIoT Device Permanent Identifier, RandN and RandD.
  properties:
    aiotDevPermId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
    randN:
      $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
    randD:
      $ref: 'TS29503_Nudm_UEAU.yaml#/components/schemas/Rand'
  required:
  - aiotDevPermId
  - randN
  - randD

GetSessionKeyResponse:
  type: object
  description: Contains the Kaiotf.
  properties:
    kAiotf:
      $ref: '#/components/schemas/Kaiotf'
  required:
  - kAiotf

```

```
GetTidRequest:
  type: object
  description: Contains a AIoT Device Permanent Identifier and Resynchronization Indicator.
  properties:
    aiotDevPermId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/AiotDevPermId'
    resyncInd:
      type: boolean
  required:
  - aiotDevPermId
```

```
GetTidResponse:
  type: object
  description: Contains T-ID Handling Info and T-ID.
  properties:
    tidHandInfo:
      $ref: 'TS29369_Nadm_DM.yaml#/components/schemas/TidHandlingInformation'
    tid:
      $ref: 'TS29369_Nadm_DM.yaml#/components/schemas/Tid'
    tidPrevious:
      $ref: 'TS29369_Nadm_DM.yaml#/components/schemas/Tid'
  required:
  - tid
  - tidHandInfo
```

```
#
# SIMPLE TYPES
#
```

```
Kaiotf:
  description: Indicates the Kaiotf.
  type: string
  pattern: '^[A-Za-f0-9]{32}$'
```

```
#
# ENUMS
#
```

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Re v	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
2025-12	CT#110	CP-253160	0001		D	Editorial Correction	19.1.0
2025-12	CT#110	CP-253160	0002	1	F	Remove the incorrect NF consumer	19.1.0
2025-12	CT#110	CP-253160	0003		F	Correction of OpenAPI	19.1.0
2025-12	CT#110	CP-253160	0004	1	F	Missing HTTP Response Code	19.1.0
2025-12	CT#110	CP-253160	0005	7	B	AIoT support for T-IDs	19.1.0
2025-12	CT#110	CP-253190	0008	3	B	New ADM security service	19.1.0
2025-12	CT#110	CP-253226	0014	3	B	Support T-ID handling information	19.1.0
2025-12	CT#110	CP-253154	0015	2	F	Correction of attribute presence	19.1.0
2025-12	CT#110	CP-253167	0016		F	29.369 Rel-19 API version and External doc update	19.1.0
2026-03	CT#111	CP-260036	0017	1	F	Correction on T-ID	19.2.0
2026-03	CT#111	CP-260036	0018		F	Add the descriptions	19.2.0
2026-03	CT#111	CP-260036	0019		D	Editorial Corrections	19.2.0
2026-03	CT#111	CP-260036	0020	1	F	Update on OpenAPI for get-rand	19.2.0
2026-03	CT#111	CP-260036	0021		F	Update on RandGetResponse	19.2.0
2026-03	CT#111	CP-260036	0022	1	F	Update on security parts	19.2.0
2026-03	CT#111	CP-260036	0023	1	F	Update on the length of Kaiotf	19.2.0
2026-03	CT#111	CP-260036	0025	2	F	Add bundled AIoT Device Profile Data retrieval and update procedures	19.2.0
2026-03	CT#111	CP-260036	0027	1	F	Make permanent ID a conditional parameter in Authentication_Get response	19.2.0
2026-03	CT#111	CP-260036	0029		F	Correction for supporting paging all	19.2.0
2026-03	CT#111	CP-260036	0031		F	Nadm_SecTID_Get correction	19.2.0
2026-03	CT#111	C4-260400	0032		F	29.369 Rel-19 API version and External doc update	19.2.0

History

Version	Date	Status
V19.0.0	January 2026	Publication
V19.1.0	February 2026	Publication
V19.2.0	March 2026	Publication