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

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

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:

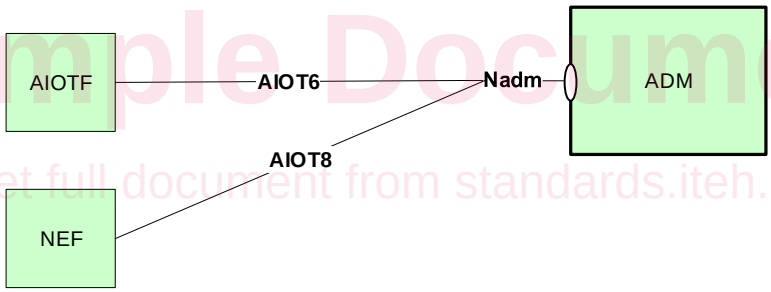

Figure 4-1: Reference model – ADM

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]).

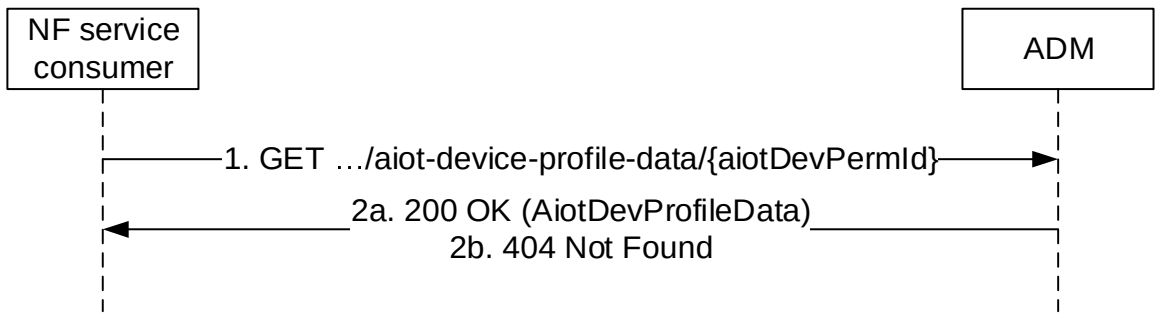

Figure 5.2.2.2.2-1: Requesting AIoT Device Profile Data

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]).

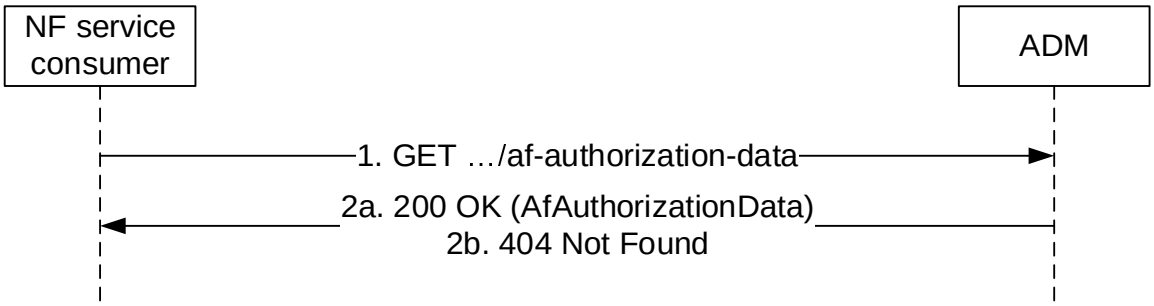

Figure 5.2.2.2.3-1: Requesting AF Authorization Data

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]).

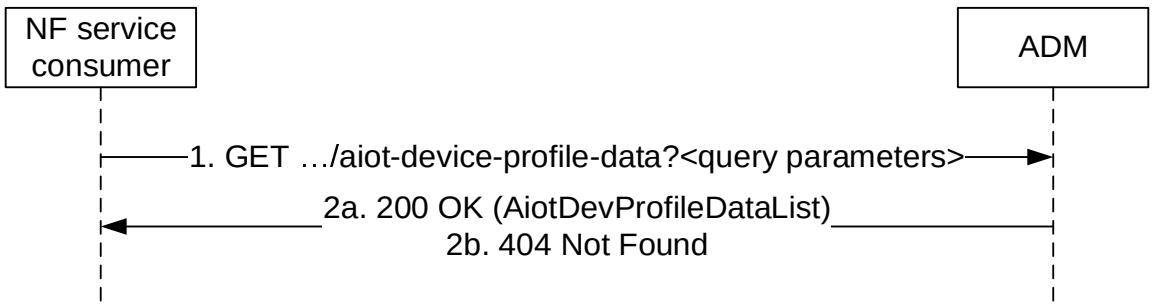

Figure 5.2.2.2.4-1: Requesting AIoT Device Profile Data for bundled AIoT Devices

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.

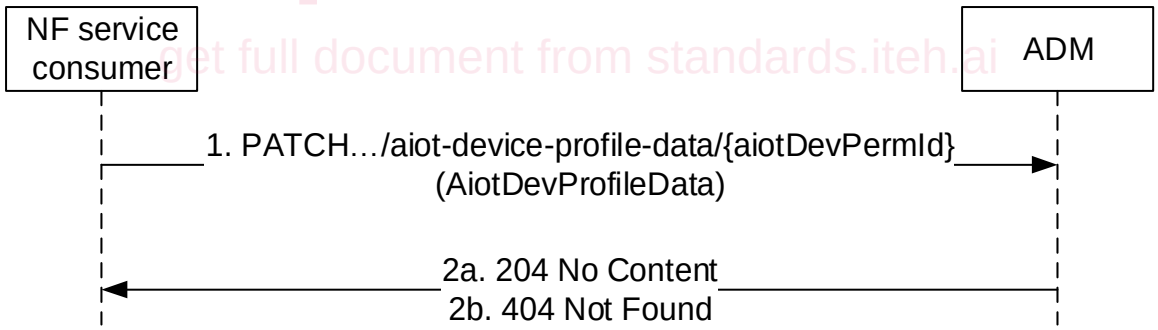

Figure 5.2.2.3.2-1: Updating AIoT Device Profile Data

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.

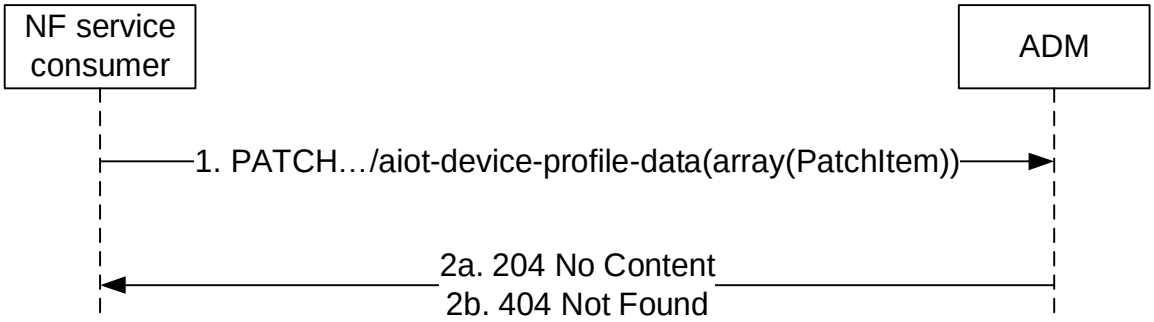

Figure 5.2.2.3.3-1: Updating AIoT Device Profile Data for bundled AIoT Devices

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]).

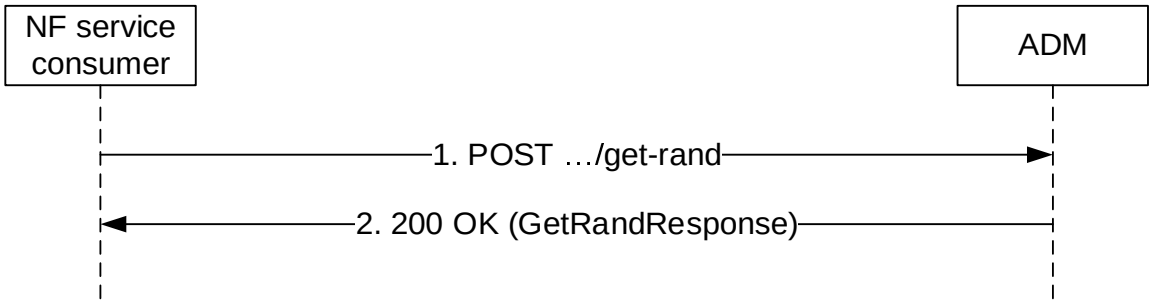

Figure 5.3.2.2.2-1: RAND Retrieval

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]).

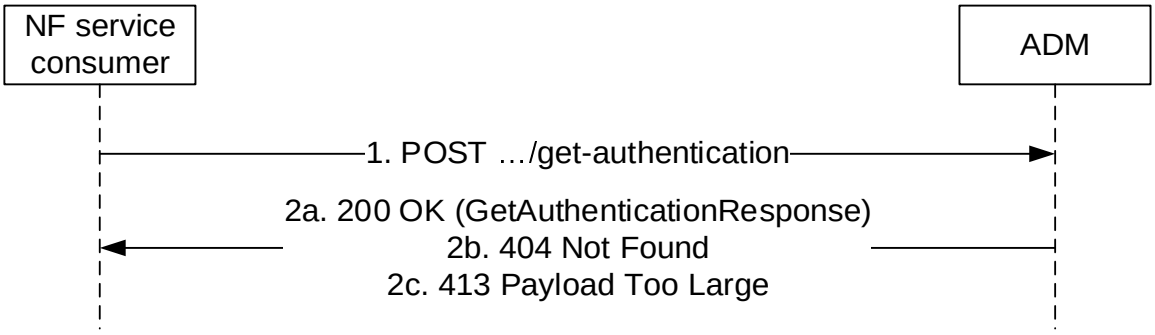

Figure 5.3.2.3.2-1: Authentication Data Retrieval

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.