

# ETSI TS 129 570 V19.2.0 (2026-03)



**5G;  
5G System;  
Service Communication Proxy Services;  
Stage 3  
(3GPP TS 29.570 version 19.2.0 Release 19)**



---

**Reference**

RTS/TSGC-0429570vj20

---

**Keywords**

5G

**ETSI**

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

---

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

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

---

**Important notice**

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

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

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

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

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

---

**Notice of disclaimer & limitation of liability**

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

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

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

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

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

---

**Copyright Notification**

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

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

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

© ETSI 2026.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

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

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

## Trademarks

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

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

---

# Legal Notice

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

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

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

---

# Modal verbs terminology

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

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

# Contents

Intellectual Property Rights .....	2
Legal Notice .....	2
Modal verbs terminology.....	2
Foreword.....	5
1 Scope .....	7
2 References .....	7
3 Definitions, symbols and abbreviations .....	8
3.1 Definitions .....	8
3.2 Abbreviations .....	8
4 Overview .....	8
4.1 Introduction .....	8
5 Services offered by the SCP .....	8
5.1 Introduction .....	8
5.2 Nscp_EventExposure Service .....	9
5.2.1 Service Description.....	9
5.2.1.1 General .....	9
5.2.1.2 Events supported by the service .....	9
5.2.2 Service Operations.....	10
5.2.2.1 Introduction.....	10
5.2.2.2 Subscribe .....	10
5.2.2.2.1 General .....	10
5.2.2.2.2 Creation of a subscription.....	10
5.2.2.2.3 Modification of a subscription.....	11
5.2.2.3 Unsubscribe.....	11
5.2.2.3.1 General .....	11
5.2.2.4 Notify .....	12
5.2.2.4.1 General .....	12
6 API Definitions .....	12
6.1 Nscp_EventExposure Service API.....	12
6.1.1 Introduction.....	12
6.1.2 Usage of HTTP .....	13
6.1.2.1 General .....	13
6.1.2.2 HTTP standard headers .....	13
6.1.2.2.1 General .....	13
6.1.2.2.2 Content type .....	13
6.1.2.3 HTTP custom headers .....	13
6.1.3 Resources.....	13
6.1.3.1 Overview.....	13
6.1.3.2 Resource: subscriptions (Collection).....	14
6.1.3.2.1 Description .....	14
6.1.3.2.2 Resource Definition.....	14
6.1.3.2.3 Resource Standard Methods .....	14
6.1.3.3 Resource: subscriptionId (Document).....	15
6.1.3.3.1 Description .....	15
6.1.3.3.2 Resource Definition.....	15
6.1.3.3.3 Resource Standard Methods .....	16
6.1.4 Custom Operations without associated resources .....	17
6.1.4.1 Overview.....	17
6.1.5 Notifications .....	17
6.1.5.1 General .....	17
6.1.5.2 SCP Event Exposure Notification .....	18
6.1.5.2.1 Description .....	18

6.1.5.2.2	Target URI.....	18
6.1.5.2.3	Standard Methods.....	18
6.1.6	Data Model .....	19
6.1.6.1	General .....	19
6.1.6.2	Structured data types .....	20
6.1.6.2.1	Introduction .....	20
6.1.6.2.2	Type: ScpEventExposureSubscription .....	20
6.1.6.2.3	Type: ScpEventExposureNotification .....	21
6.1.6.2.4	Type: ScpEventExposureSubsResp.....	21
6.1.6.2.5	Type: ScpEventFilter.....	21
6.1.6.2.6	Type: ScpEventReport.....	22
6.1.6.2.7	Type: FailureCauseOccurrence .....	22
6.1.6.2.8	Type: ScpSignallingInfo.....	23
6.1.6.2.9	Type: ScpEventFilterConfig.....	26
6.1.6.2.10	Type: ReselectionStat.....	28
6.1.6.3	Simple data types and enumerations .....	28
6.1.6.3.1	Introduction .....	28
6.1.6.3.2	Simple data types.....	28
6.1.6.3.3	Enumeration: FailureCause .....	28
6.1.6.3.4	Enumeration: ScpEventType .....	29
6.1.6.3.5	Enumeration: ReselectionReason .....	29
6.1.6.3.6	Enumeration: ConnectionStatus .....	29
6.1.7	Error Handling .....	29
6.1.7.1	General .....	29
6.1.7.2	Protocol Errors .....	29
6.1.7.3	Application Errors .....	29
6.1.8	Feature negotiation .....	30
6.1.9	Security .....	30
6.1.10	HTTP redirection .....	30
<b>Annex A (normative): OpenAPI specification .....</b>		<b>31</b>
A.1	General .....	31
A.2	Nscp_EventExposure API.....	31
<b>Annex B (informative): Change history .....</b>		<b>38</b>
History .....		39

---

# 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 Nscp Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the SCP.

The 5G System stage 2 architecture and procedures are specified in TS 23.501 [2], TS 23.288 [14], and TS 23.502 [3].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in TS 29.500 [4] and 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 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".
- [15] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".
- [16] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".
- [17] 3GPP TS 29.122: "T8 reference point for Northbound APIs".
- [18] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

---

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 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 23.501 [2] and the following apply. An abbreviation defined in the present document or 3GPP TS 23.501 [2] takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1]. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TS 23.501 [2].

SCP	Service Communication Proxy
-----	-----------------------------

---

## 4 Overview

### 4.1 Introduction

Within the 5GC, the SCP offers services to the NWDAF and DCCF via the Nscp service based interface (see 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 23.288 [14]).

Figure 4.1-1 provides the reference model (in service based interface representation and in reference point representation), with focus on the SCP and the scope of the present specification.

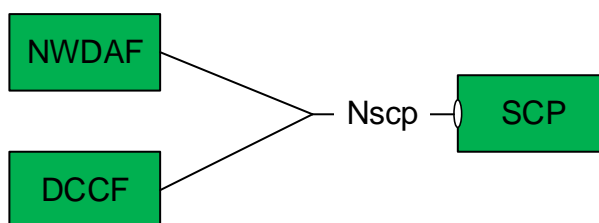


Figure 4.1-1: Reference model – SCP

---

## 5 Services offered by the SCP

### 5.1 Introduction

The table 5.1-1 shows the SCP services and SCP service operations:

Table 5.1-1 List of SCP Services

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nscp_EventExposure	Subscribe	Subscribe/Notify	NWDAF, DCCF
	Unsubscribe	Subscribe/Notify	NWDAF, DCCF
	Notify	Subscribe/Notify	NWDAF, DCCF

Table 5.1-2 summarizes the corresponding APIs defined for this specification.

Table 5.1-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
Nscp_EventExposure	6.1	SCP Event Exposure Service	TS29570_Nscp_EventExposure.yaml	nscp-ee	A.2

## 5.2 Nscp\_EventExposure Service

### 5.2.1 Service Description

#### 5.2.1.1 General

The Nscp\_EventExposure service enables the SCP to expose real-time event data related to network signaling and performance to other NFs (e.g. NWDAF and DCCF) for analytics and monitoring.

#### 5.2.1.2 Events supported by the service

The following event type(s) are supported by the Nscp\_EventExposure Service:

Event: SERVICE\_SIGNALLING\_CHARACTERISTICS:

An NF subscribes to this event type to receive the SCP reports of the observed rate (i.e. number per time interval) of several types of signalling messages received and sent by NF instance(s) or NF service instance(s), the percentage of failed transactions, NF or NF service overload control information, SCP reselection reasons, NF service connection status, and various delay and performance metrics.

This event implements the "Service Signalling Characteristics Information" as described in clause 5.2.29 of 3GPP TS 23.502 [3] and Table 6.22.2-8 of 3GPP TS 23.288 [14].

Target: NF type, NF service instance, NF instance, NF set or NF service name.

Report Type: Periodic Report, One-Time Report.

Input in the subscription: target ID, optional filters, e.g. reporting threshold (in terms of absolute transaction or deviation from average, or in terms of a minimum percentage failed transactions), time window.

Notification: Event type, time stamp, and optionally: one or more of the following types of information:

- Per NF instance, See Table 6.22.2-8 of 3GPP TS 23.288 [14].
  - Number of successful responses related to SCP egress interface associated to their initial requests during a time interval.
  - Number of failed responses related to SCP egress interface associated to their initial requests during a time interval.
  - Distribution of reasons for failed responses related to SCP egress interface associated to their initial requests, e.g. the number of failed responses due to time-outs, the number of failed responses due to server errors, the number of failed responses due to consumer errors.

- Connection status: The connection status between SCP and NF service instance.
- SCP reselection statistics: Reselection reasons with their occurrence counts.
- Overload control information indicating the current overload of the NF and NF Service(s).
- Average response time: Average time taken to get response from NF service instance after SCP sent the request.

## 5.2.2 Service Operations

### 5.2.2.1 Introduction

The Nscp\_EventExposure service defines three service operations:

- Notify: The SCP sends notifications to subscribed consumers, providing event data and related information.
- Subscribe: A network function (NF) subscribes to receive notifications for specific events, with the option to define filtering or subscription parameters.
- Unsubscribe: An NF unsubscribes from a previously established event notification subscription.

These operations allow consumers to manage the receipt of event data related to network signaling and performance.

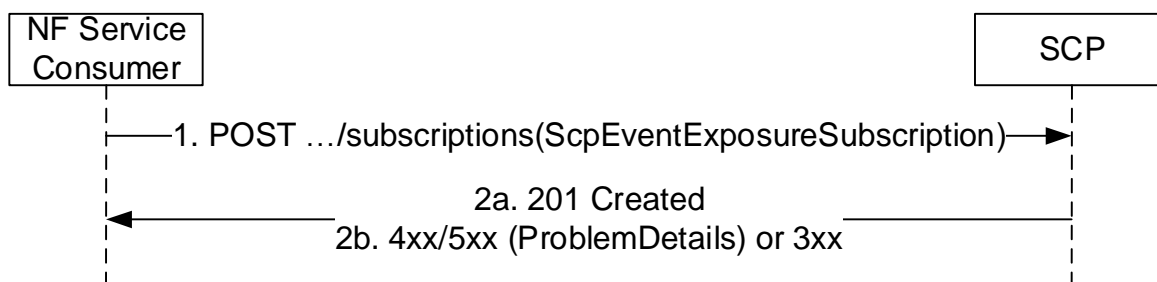
### 5.2.2.2 Subscribe

#### 5.2.2.2.1 General

See Table 5.1-1 for an overview of the service operations supported by the Nscp\_EventExposure service.

#### 5.2.2.2.2 Creation of a subscription

This procedure allows NF Service Consumer to subscribe by using HTTP POST method with the URI of subscriptions collection.



**Figure 5.2.2.2.2-1: Subscription of NF service consumer to SCP Event Exposure**

1. The NF Service Consumer shall send an HTTP POST request to the resource URI associated with the subscription collection.
- 2a. On success, "201 Created" shall be returned. The response body shall include a HTTP Location header including the subscription ID together with the status code 201 indicating the requested resource is created in the response message.
- 2b. On failure or redirection, one of the HTTP status codes listed in Table 6.1.3.2.3.1-3 shall be returned. For a 4xx/5xx response, the message body should contain a ProblemDetails structure indicating appropriate additional error information.

5.2.2.2.3 Modification of a subscription

This procedure allows NF Service Consumer to modify an existing subscription by using HTTP PATCH method with the URI of the individual subscription resource.

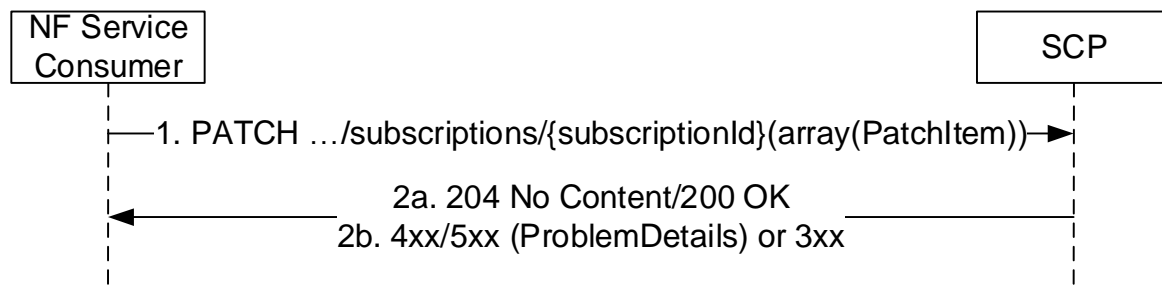


Figure 5.2.2.2.3-1: Modification of subscription for SCP Event Exposure

1. The NF Service Consumer shall send a PATCH request to modify a subscription resource in the SCP.

2a. On success,

"204 No Content" shall be returned, if there is no payload in the response. If the request included an expiry time and "204 No Content" is returned, it indicates that the SCP has accepted the requested expiry time.

"200 OK" shall be returned and include a response body of type ScpEventExposureSubsResp if a payload needs to be returned. When returning a "200 OK" response, if the request included an expiry time, then the response based on operator policies and taking into account the expiry time included in the request, shall contain an expiry time (i.e. a future timestamp), as determined by the SCP, after which the subscription becomes invalid. If an expiry time was included in the request, then the expiry time returned in the response should be less than or equal to that value.

NOTE: In this release of the specification, the payload contains only one item, i.e. expiry time. In this release, if the expiry time included is in the request and the expiry time determined by SCP is equal to the value of the expiry time in the request, a payload is not needed to be returned and "204 No Content" is returned.

2b. On failure or redirection, one of the HTTP status codes listed in Table 6.1.3.3.3.1-3 shall be returned. For a 4xx/5xx response, the message body contains a ProblemDetails structure indicating appropriate additional error information.

5.2.2.3 Unsubscribe

5.2.2.3.1 General

This procedure allows NF Service Consumer to delete an existing subscription by using the HTTP DELETE method with the URI of the individual subscription resource to be deleted.

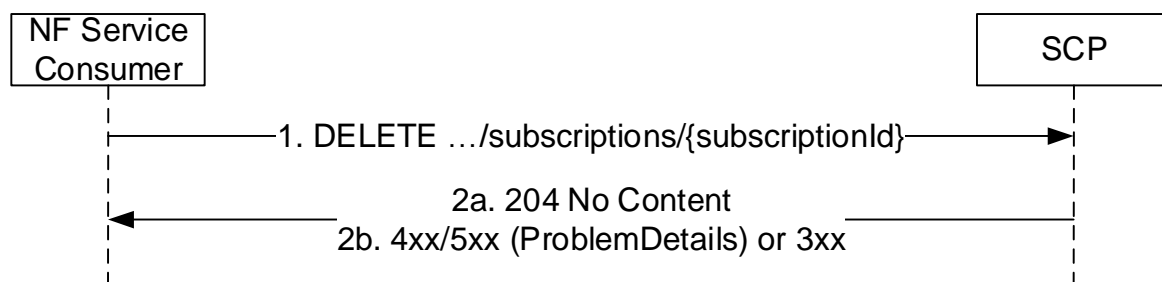


Figure 5.2.2.3.1-1: Unsubscribe Service Operation for SCP Event Exposure

1. The NF consumer shall send a DELETE request to the SCP to delete the subscription.

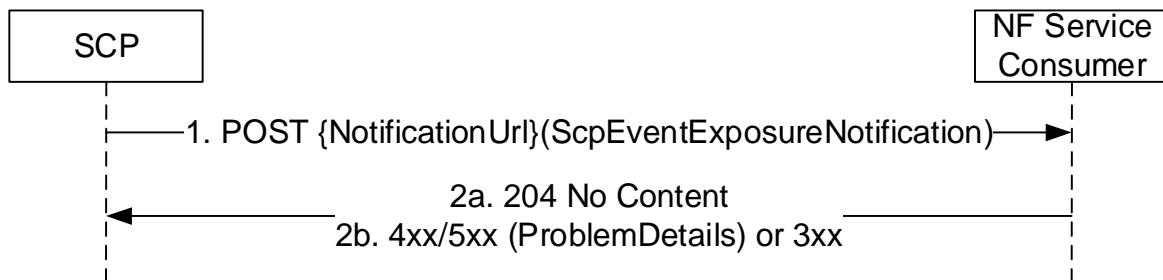
2a. On success, "204 No content" shall be returned by the NF Service Consumer.

- 2b. On failure or redirection, one of the appropriate HTTP status codes listed in Table 6.1.3.3.2-3 shall be returned. For a 4xx/5xx response, the message body should contain a ProblemDetails structure indicating appropriate additional error information.

## 5.2.2.4 Notify

### 5.2.2.4.1 General

The Notify service operation is used to allow the NF service consumer to get notifications from SCP.



**Figure 5.2.2.4.1-1: Notification for SCP Event Exposure**

1. The SCP shall send a POST request to the NF Service Consumer with the information on Notification target address. The request body shall include Event specific parameters and notification correlation ID, if received.

- 2a. On success, "204 No content" shall be returned by the NF Service Consumer.

2b. On failure or redirection, one of the appropriate HTTP status codes listed in Table 6.1.5.2.3.1-2 shall be returned. For a 4xx/5xx response, the message body should contain a ProblemDetails structure indicating appropriate additional error information.

---

## 6 API Definitions

### 6.1 Nscp\_EventExposure Service API

#### 6.1.1 Introduction

The Nscp\_EventExposure shall use the Nscp\_EventExposure API.

The API URI of the Nscp\_EventExposure 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 "nscp-ee".
- 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 Nscp\_ee 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

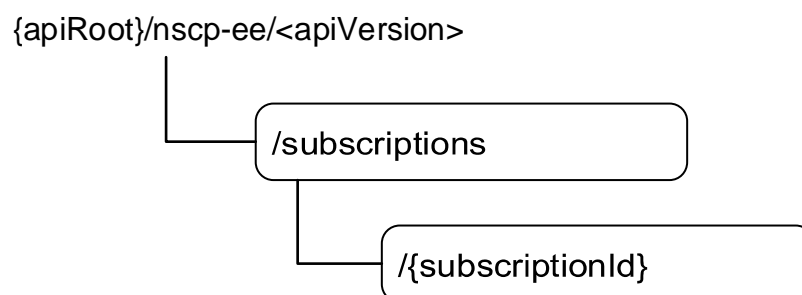
The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

## 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 Nscp\_EventExposure API.



**Figure 6.1.3.1-1: Resource URI structure of the Nscp\_EventExposure 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)
subscriptions (Collection)	/subscriptions	POST	Mapped to the service operation subscribe, when to create a subscription
subscriptionId (Document)	/subscriptions/{subscriptionId}	PATCH	Modify the subscription identified by {subscriptionId}
		DELETE	Delete the subscription identified by {subscriptionId}

### 6.1.3.2 Resource: subscriptions (Collection)

#### 6.1.3.2.1 Description

This resource represents a collection of subscriptions created by NF service consumers of Nscp\_EventExposure service.

This resource is modelled as the Collection resource archetype (see clause C.2 of 3GPP TS 29.501 [5]).

#### 6.1.3.2.2 Resource Definition

Resource URI: {apiRoot}/nscp-ee/<apiVersion>/subscriptions 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

#### 6.1.3.2.3 Resource Standard Methods

##### 6.1.3.2.3.1 POST

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 POST 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 POST Request Body on this resource**

Data type	P	Cardinality	Description
ScpEventExposureSubscription	M	1	SCP Event Exposure Subscription to be created

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

Data type	P	Cardinality	Response codes	Description
ScpEventExposureSubsResp	M	1	201 Created	Represents successful creation of an SCP Subscription
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection.
NOTE: The mandatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply, with response body containing an object of ProblemDetails data type (see clause 5.2.7 of 3GPP TS 29.500 [4]).				

**Table 6.1.3.2.3.1-4: Headers supported by the 201 response code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/nscp-ee/<apiVersion>/subscriptions/{subscriptionId}

**Table 6.1.3.2.3.1-5: Headers supported by the 307 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP.

**Table 6.3.3.2.3.1-6: Headers supported by the 308 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP.

### 6.1.3.3 Resource: subscriptionId (Document)

#### 6.1.3.3.1 Description

This resource represents an individual of subscription created by NF service consumers of Nscp\_EventExposure service.

This resource is modelled as the Document resource archetype (see clause C.1 of 3GPP TS 29.501 [5]).

#### 6.1.3.3.2 Resource Definition

Resource URI: {apiRoot}/nscp-ee/<apiVersion>/subscriptions/{subscriptionId}

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
subscriptionId	string	Represents the identity of a specific subscription

## 6.1.3.3.3 Resource Standard Methods

## 6.1.3.3.3.1 PATCH

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 PATCH method on this resource**

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 6.1.3.3.3.1-2 and the response data structure 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 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 subscription, according to the JSON PATCH format specified in IETF RFC 6902 [15].

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

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Represents a successful update on SCP Event Exposure Subscription
ScpEventExposureSubs Resp	M	1	200 OK	Represents successful modification of an SCP Subscription.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection.
NOTE: The mandatory HTTP error status code for the PATCH method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply, with response body containing an object of ProblemDetails data type (see clause 5.2.7 of 3GPP TS 29.500 [4]).				

**Table 6.1.3.3.3.1-4: Headers supported by the 307 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP.

**Table 6.1.3.3.3.1-5: Headers supported by the 308 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP.

## 6.1.3.3.3.2 DELETE

This method shall support the URI query parameters specified in table 6.1.3.3.3.2-1.

**Table 6.1.3.3.2-1: URI query parameters supported by the DELETE method on this resource**

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 6.1.3.3.2-2 and the response data structures and response codes specified in table 6.1.3.3.2-3.

**Table 6.1.3.3.2-2: Data structures supported by the DELETE Request Body on this resource**

Data type	P	Cardinality	Description
n/a			

**Table 6.1.3.3.2-3: Data structures supported by the DELETE Response Body on this resource**

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection.

NOTE 1: The mandatory HTTP error status code for the DELETE method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply, with response body containing an object of ProblemDetails data type (see clause 5.2.7 of 3GPP TS 29.500 [4]).

**Table 6.1.3.3.2-4: Headers supported by the 307 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP.

**Table 6.1.3.3.2-5: Headers supported by the 308 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located on an alternative service instance within the same SCP

## 6.1.4 Custom Operations without associated resources

### 6.1.4.1 Overview

There are no custom operations without associated resources supported on Nscp\_EventExposure Service.

## 6.1.5 Notifications

### 6.1.5.1 General

Notifications shall comply to clause 6.2 of 3GPP TS 29.500 [4] and clause 4.6.2.3 of 3GPP TS 29.501 [5].

**Table 6.1.5.1-1: Notifications overview**

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
SCP Event Exposure Notification	{notificationUri}	POST	

## 6.1.5.2 SCP Event Exposure Notification

### 6.1.5.2.1 Description

The Event Notification is used by the NF service producer to report one or several observed Events to a NF service consumer that has subscribed to such Notifications.

### 6.1.5.2.2 Target URI

The Callback URI "{notificationUri}" shall be used with the callback URI variables defined in table 6.1.5.2.2-1.

**Table 6.1.5.2.2-1: Callback URI variables**

Name	Definition
notificationUri	String formatted as URI with the Callback Uri

### 6.1.5.2.3 Standard Methods

#### 6.1.5.2.3.1 POST

This method shall support the request data structures specified in table 6.1.5.2.3.1-1 and the response data structures and response codes specified in table 6.1.5.2.3.1-1.

**Table 6.1.5.2.3.1-1: Data structures supported by the POST Request Body**

Data type	P	Cardinality	Description
ScpEventExposureNotification	M	1	Represents the notification to be delivered

**Table 6.1.5.2.3.1-2: Data structures supported by the POST Response Body**

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. (NOTE)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. (NOTE)
NOTE: The mandatory HTTP error status codes for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

**Table 6.1.5.2.3.1-3: Headers supported by the 307 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	A URI pointing to the endpoint of the NF service consumer to which the notification should be sent.

**Table 6.1.5.2.3.1-4: Headers supported by the 308 Response Code on this resource**

Name	Data type	P	Cardinality	Description
Location	string	M	1	A URI pointing to the endpoint of the NF service consumer to which the notification should be sent

## 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 Nscp\_EventExposure service based interface protocol.

**Table 6.1.6.1-1: Nscp\_EventExposure specific Data Types**

Data type	Clause defined	Description	Applicability
ScpEventExposureSubscription	6.1.6.2.2	Represents an event subscription resource to SCP	
ScpEventExposureNotification	6.1.6.2.3	Represents an event notification.	
ScpEventExposureSubsResp	6.1.6.2.4	Represent the SCP Event Exposure Response	
ScpEventFilter	6.1.6.2.5		
ScpEventReport	6.1.6.2.6		
FailureCauseOccurrence	6.1.6.2.7		
ScpSignallingInfo	6.1.6.2.8	SCP signalling information	
ScpEventFilterConfig	6.1.6.2.9	Event filter	
ReselectionStat	6.1.6.2.10	Reselection statistics	
FailureCause	6.1.6.3.3		
ScpEventType	6.1.6.3.4		
ReselectionReason	6.1.6.3.5	Reselection reason	
ConnectionStatus	6.1.6.3.6	Connection status	

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

Table 6.1.6.1-2: Nscp\_EventExposure re-used Data Types

Data type	Reference	Comments	Applicability
ServiceName	3GPP TS 29.510 [10]	Service Name	
NFType	3GPP TS 29.510 [10]	NF type	
DateTime	3GPP TS 29.571 [16]	Date time	
DurationSec	3GPP TS 29.571 [16]	Duration in seconds	
NfInstanceId	3GPP TS 29.571 [16]	Identifier (UUID) of the NF Instance. The hexadecimal letters of the UUID should be formatted by the sender as lower-case characters and shall be handled as case-insensitive by the receiver.	
NfSetId	3GPP TS 29.571 [16]	NF Set ID	
UInteger	3GPP TS 29.571 [16]	Unsigned Integer	
Uri	3GPP TS 29.571 [16]	URI	
OverloadControlInfo	3GPP TS 29.571 [16]	Overload Control information	
TimeWindow	3GPP TS 29.122 [17]	Time window	
RecurTime	3GPP TS 29.503 [18]	Recurring time	

## 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: ScpEventExposureSubscription

Table 6.1.6.2.2-1: Definition of type ScpEventExposureSubscription

Attribute name	Data type	P	Cardinality	Description	Applicability
eventList	array(ScpEvent Filter)	M	1..N	Describes the events to be subscribed in subscription request or the events successfully subscribed for this subscription in subscription response.	
eventNotifyUri	Uri	M	1	Identifies the recipient of notifications sent by SCP for this subscription.	
notifyCorrelationId	string	M	1	Identifies the notification correlation ID. The SCP shall include this ID in the notifications. The value of this IE shall be unique per subscription for a given NF service consumer.	
expiry	DateTime	O	0..1	When present, this IE shall represent the UTC time after which the subscribed event(s) shall stop generating report and the subscription becomes invalid.	

## 6.1.6.2.3 Type: ScpEventExposureNotification

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

Attribute name	Data type	P	Cardinality	Description	Applicability
notifyCorrelationId	string	M	1	This IE shall indicate the notification correlation Id provided by the NF service consumer during event subscription. This parameter can be useful if the NF service consumer uses a common call-back URI for multiple subscriptions.	
reportList	array(ScpEvent Report)	C	1..N	This IE shall be present if an event is reported. When present, this IE represents the event reports to be delivered.	

## 6.1.6.2.4 Type: ScpEventExposureSubsResp

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

Attribute name	Data type	P	Cardinality	Description	Applicability
expiryTime	DateTime	C	0..1	When present, it shall indicate the expiration time of the subscription, as determined by the operator's policy. The NF consumer shall renew or re-subscribe before expiration if continued event notifications are required.  The IE shall be present in the response to a subscription request or a modification request, if the request included an expiry time and the SCP determines a different expiry time for the subscription. It may be present otherwise.	

## 6.1.6.2.5 Type: ScpEventFilter

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

Attribute name	Data type	P	Cardinality	Description	Applicability
eventType	ScpEventType	M	1	The SCP event type to be reported.	
timeWindow	RecurTime	O	0..1	When present, it shall indicate the data collection window.	
filterConfigs	array(ScpEvent FilterConfig)	O	1..N	List of filter configurations associated with this eventType.	

## 6.1.6.2.6 Type: ScpEventReport

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

Attribute name	Data type	P	Cardinality	Description	Applicability
eventType	ScpEventType	M	1	Indicates the type of the event which triggers the report.	
timeStamp	DateTime	M	1	This IE shall indicate the time in UTC when the event report was generated.	
scpSignallingInfoList	array(ScpSignallingInfo)	O	1..N	Per-service instance statistics including SCP/NF behavior and overload. See table 6.22.2-8 of 3GPP TS 23.288 [14] and clause 5.2.29 of 3GPP TS 23.502 [3].	

## 6.1.6.2.7 Type: FailureCauseOccurrence

**Table 6.1.6.2.7-1: Definition of type FailureCauseOccurrence**

Attribute name	Data type	P	Cardinality	Description	Applicability
cause	FailureCause	M	1	Reasons of failed responses of NF Service(s).	
count	UInteger	M	1	Number of the failed responses due to the reason provided in "cause".	

6.1.6.2.8 Type: ScpSignallingInfo

**Table 6.1.6.2.8-1: Definition of type ScpSignallingInfo**

Attribute name	Data type	P	Cardinality	Description	Applicability
serviceInstanceid	string	C	0..1	This IE shall be present if available. When present it shall identify the NF service instance for which the statistics are reported. (NOTE)	
nfInstanceid	NfInstanceid	C	0..1	NF Instance ID hosting the NF service instance. The IE shall be present when available. (NOTE)	
serviceName	ServiceName	O	0..1	Identifies the name of the NF service (e.g., Namf-Comm, Nudm-SDM) for which the statistics apply. (NOTE)	
nfType	NFType	O	0..1	Identifies the NF type of The NF instance for which the statistics are reported. (NOTE)	
nfSetid	NfSetid	O	0..1	Identifies the NF set of the NF instance for which the statistics are reported. (NOTE)	
rcvRequestCount	UInteger	O	0..1	Number of requests received by SCP from the NF service instance.	
sentRequestCount	UInteger	O	0..1	Number of requests sent by the SCP to the NF service instance.	
successfulResponseCount	UInteger	O	0..1	Number of successful responses received from this NF service instance.	
failureResponseCount	UInteger	O	0..1	Total number of failed responses received from this NF service instance.	
failureCauseStats	array(FailureCauseOccurrence)	O	1..N	Breakdown of failure causes for this NF service instance.	
scpFailureCount	UInteger	O	0..1	Number of failures generated by the SCP before reaching the NF (e.g. unreachable NF).	
scpFailureCauseStats	array(FailureCauseOccurrence)	O	0..1	Breakdown of SCP-side failure causes targeting this NF service instance.	
reselectionCount	UInteger	O	0..1	Number of times SCP reselect NF instance	
reselectionStatList	array(ReselectionStat)	O	1..N	List of reasons of SCP reselecting NF instance producer with their occurrence counts. Each entry pairs a ReselectionReason with the corresponding number of reselections performed by the SCP.	
connectionStatus	ConnectionStatus	O	0..1	Connection status between SCP and the NF service instance (e.g., ACTIVE, INACTIVE).	
avgResponseTimeToNF	UInteger	O	0..1	Average time in units of milliseconds between SCP sending the request to the NF instance and SCP receiving the response from the NF instance. The requests for which no response from the NF instance is received are ignored for calculating the average time in this IE.	
overloadControlInfo	OverloadControlInfo	O	0..1	Contains overload control metrics (e.g., reduction percentage, validity period) for the reported NF service instance, as defined in clause 6.4 and 5.2.3.2.9 of 3GPP TS 29.500 [4]. The SCP may send this information based on the 3gpp-Sbi-Oci header when overload mitigation is active towards the NF (service) instance.	

NOTE: At least one of the following identifiers serviceInstanceId, nfInstanceId, serviceName, nfType or nfSetId shall be present.

6.1.6.2.9 Type: ScpEventFilterConfig

**Table 6.1.6.2.9-1: Definition of type ScpEventFilterConfig**

Attribute name	Data type	P	Cardinality	Description
nfType	NFType	O	0..1	When present, this IE shall indicate the type of target NF for which the event is subscribed.  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
targetNfSetId	NfSetId	O	0..1	When present, this IE shall contain the identifier of the target NF Set for the event reports.  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
targetNfIdList	array(NfInstanceId)	O	1..N	When present, this IE shall contain the NF instance identifiers of the target NFs for the event report.  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
serviceNameList	array(ServiceName)	O	1..N	When present, it shall indicate the NF service name(s) for which the event will be reported.  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
serviceInstanceIdList	array(string)	O	1..N	When present, it shall indicate the NF service instance(s) for which the event will be reported.  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
reportingThreshold	UInteger	O	0..1	This IE shall indicate the threshold on the number of transactions for reporting.  When present in the subscription request, it indicates that the subscriber requests a report when the number of transactions exceeds this absolute threshold,  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".
devFromAveTh	UInteger	O	0..1	This IE shall indicate the threshold on deviation from average number of the transactions for reporting.  When present in the subscription request, it indicates that the subscriber requests a report when the difference of the number of transactions with the average number of transactions exceeds this threshold,  This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".

failureTh	UInteger	O	0..1	<p>This IE shall indicate the threshold on percentage of failure events for reporting.</p> <p>When present in the subscription request, it indicates that the subscriber requests a report when percentage of failure transactios exceeds this threshold,</p> <p>This IE may be present if the eventType is "SERVICE_SIGNALLING_CHARACTERISTIC S".</p>
-----------	----------	---	------	--

6.1.6.2.10 Type: ReselectionStat

**Table 6.1.6.2.10-1: Definition of type ReselectionStat**

Attribute name	Data type	P	Cardinality	Description	Applica bility
reselectionReason	ReselectionReason	M	1	Reason for SCP reselection of an NF service instance, as defined in clause 6.3.1.0 of 3GPP TS 23.501 [2].	
count	UInteger	M	1	Number of times the SCP performed reselection due to the given reason within the reporting interval.	

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
n/a			

6.1.6.3.3 Enumeration: FailureCause

**Table 6.1.6.3.3-1: Enumeration FailureCause**

Enumeration value	Description
"TIME_OUT"	Time-out
"SERVER_ERROR"	Server error
"CLIENT_ERROR"	Client error
"OTHER_FAILURE_REASONS"	Other failure reasons which are not explicitly listed

## 6.1.6.3.4 Enumeration: ScpEventType

**Table 6.1.6.3.4-1: Enumeration ScpEventType**

Enumeration value	Description
"SERVICE_SIGNALLING_CHARACTERISTICS"	An NF subscribes to this event to receive the SCP reports of the observed rate of different types of signalling messages received and sent by different NF instance(s), the percentage of failed transactions, as described in clause 5.2.29.2.1 of 3GPP TS 23.502 [3].

## 6.1.6.3.5 Enumeration: ReselectionReason

**Table 6.1.6.3.5-1: Enumeration ReselectionReason**

Enumeration value	Description
"TARGET_NF_UNREACHABLE"	The original NF instance could not be reached due to network or service unavailability.
"LOAD_BASED_RESELECTION"	The reselection was triggered due to overload or high load conditions on the target NF instance.
"SERVICE_INSTANCE_FAILURE"	The reselection occurred due to a failure at the specific NF service instance (e.g., timeout or repeated failed transactions).
"UNSPECIFIED"	For any reason not covered by an explicit value above.

## 6.1.6.3.6 Enumeration: ConnectionStatus

**Table 6.1.6.3.6-1: Enumeration ConnectionStatus**

Enumeration value	Description
"ACTIVE"	The SCP currently has an active connection to the NF service instance.
"INACTIVE"	The SCP currently does not have an active connection to the NF service instance.

## 6.1.7 Error Handling

## 6.1.7.1 General

For the Nscp\_EventExposure API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Nscp\_EventExposure API.

## 6.1.7.2 Protocol Errors

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

## 6.1.7.3 Application Errors

The application errors defined for the Nscp\_EventExposure service are listed in Table 6.1.7.3-1.

**Table 6.1.7.3-1: Application errors**

Application Error	HTTP status code	Description
n/a		

## 6.1.8 Feature negotiation

The optional features in table 6.1.8-1 are defined for the Nscp\_EventExposure 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
n/a		

## 6.1.9 Security

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

The Nscp\_EventExposure API defines scopes for OAuth2 authorization as specified in 3GPP TS 33.501 [8];

**Table 6.1.9-1: OAuth2 scopes defined in Nscp\_EventExposure API**

Scope	Description
"nscp-ee"	Access to the Nscp_EventExposure API.

## 6.1.10 HTTP redirection

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

An SCP that reselects a different SCP producer instance will return the NF Instance ID of the new SCP 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 SCP redirects a service request to a different SCP using an 307 Temporary Redirect or 308 Permanent Redirect status code, the identity of the new SCP 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 Nscp\_EventExposure API

```

openapi: 3.0.0
info:
  title: Nscp_EventExposure
  version: 1.0.1
  description: |
    SCP Event Exposure Service.
    © 2026, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
externalDocs:
  description: 3GPP TS 29.570 V19.2.0; Service Communication Proxy Services.
  url: http://www.3gpp.org/ftp/Specs/archive/29_series/29.570/
servers:
  - url: '{apiRoot}/nscp-ee/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501
security:
  - {}
  - oAuth2ClientCredentials:
    - nscp-ee
paths:
  /subscriptions:
    post:
      summary: Nscp_EventExposure Subscribe service Operation
      tags:
        - Subscriptions(Collection)
      operationId: CreateSubscription
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ScpEventExposureSubscription'
            required: true
      responses:
        '201':
          description: Subscription Created
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure
                {apiRoot}/nscp-ee/<apiVersion>/subscriptions/{subscriptionId}
              required: true
              schema:
                type: string
          content:

```

```

    application/json:
      schema:
        $ref: '#/components/schemas/ScpEventExposureSubsResp'
  '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'
  '501':
    $ref: 'TS29571_CommonData.yaml#/components/responses/501'
  '502':
    $ref: 'TS29571_CommonData.yaml#/components/responses/502'
  '503':
    $ref: 'TS29571_CommonData.yaml#/components/responses/503'
  default:
    $ref: 'TS29571_CommonData.yaml#/components/responses/default'
callbacks:
  onScpEventExposureNotification:
    '{$request.body#/subscription/notificationUri}':
      post:
        summary: SCP Event Exposure Notification
        requestBody:
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ScpEventExposureNotification'
            required: true
        responses:
          '204':
            description: Successful acknowledgement
          '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:
            $ref: 'TS29571_CommonData.yaml#/components/responses/default'
/subscriptions/{subscriptionId}:
  patch:

```

```

summary: Nscp_EventExposure Subscribe Modify service Operation
tags:
  - Individual subscription (Document)
operationId: ModifySubscription
parameters:
  - name: subscriptionId
    in: path
    required: true
    description: Unique ID of the subscription to be modified
    schema:
      type: string
requestBody:
  content:
    application/json-patch+json:
      schema:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PatchItem'
        minItems: 1
      required: true
responses:
  '200':
    description: Subscription modified successfully
    content:
      application/json:
        schema:
          $ref: '#/components/schemas/ScpEventExposureSubsResp'
  '204':
    description: Expected response to a successful subscription modification
  '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'
  '501':
    $ref: 'TS29571_CommonData.yaml#/components/responses/501'
  '502':
    $ref: 'TS29571_CommonData.yaml#/components/responses/502'
  '503':
    $ref: 'TS29571_CommonData.yaml#/components/responses/503'
  default:
    description: Unexpected error

delete:
summary: Nscp_EventExposure Unsubscribe service Operation
tags:
  - Individual subscription (Document)
operationId: DeleteSubscription
parameters:
  - name: subscriptionId
    in: path
    required: true
    description: Deletion of Subscription
    schema:
      type: string
responses:
  '204':
    description: Subscription deleted successfully
  '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

```

```

components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nscp-ee: Access to the Nscp_EventExposure API

```

```

  schemas:
  #
  # STRUCTURED TYPES
  #

```

```

ScpEventExposureSubscription:
  description: Describes an event to be subscribed
  type: object
  properties:
    eventList:
      type: array
      items:
        $ref: '#/components/schemas/ScpEventFilter'
      minItems: 1
    eventNotifyUri:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
    notifyCorrelationId:
      type: string
    expiry:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
  required:
  - eventList
  - eventNotifyUri
  - notifyCorrelationId

```

```

ScpEventFilter:
  description: Describes an SCP event
  type: object
  properties:
    eventType:
      $ref: '#/components/schemas/ScpEventType'
    timeWindow:
      $ref: 'TS29503_Nudm_SDM.yaml#/components/schemas/RecurTime'
    filterConfigs:
      type: array
      items:
        $ref: '#/components/schemas/ScpEventFilterConfig'
      minItems: 1
  required:
  - eventType

```

```

ScpEventFilterConfig:
  description: Describes an SCP event filters
  type: object
  properties:
    nfType:
      $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/NFType'
    targetNfSetId:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSetId'
    targetNfIdList:
      type: array
      items:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
      minItems: 1
    serviceNameList:
      type: array
      items:
        $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/ServiceName'
      minItems: 1
    serviceInstanceIdList:
      type: array
      items:
        type: string
      minItems: 1
    reportingThreshold:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
    devFromAveTh:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
    failureTh:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'

ScpEventExposureNotification:
  description: Represents an event notification
  type: object
  properties:
    notifyCorrelationId:
      type: string
    reportList:
      type: array
      items:
        $ref: '#/components/schemas/ScpEventReport'
      minItems: 1

ScpEventExposureSubsResp:
  description: Represents SCP Event Exposure Subscription Response
  type: object
  properties:
    expiryTime:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'

ScpEventReport:
  description: Describes an SCP report triggered due to a subscription to an SCP event
  type: object
  properties:
    eventType:
      $ref: '#/components/schemas/ScpEventType'
    timeStamp:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
    scpSignallingInfoList:
      type: array
      items:
        $ref: '#/components/schemas/ScpSignallingInfo'
      minItems: 1
  required:
    - eventType
    - timeStamp

FailureCauseOccurrence:
  description: The number of times that a failure happened due to a particular cause
  type: object
  properties:

```

```

cause:
  $ref: '#/components/schemas/FailureCause'
count:
  $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
required:
- cause
- count

```

```

ScpSignallingInfo:
description:
  Per service instance statistics including SCP and NF statistics behavior and overload.
type: object
properties:
  serviceInstanceId:
    type: string
  nfInstanceId:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
  serviceName:
    $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/ServiceName'
  nfType:
    $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/NFType'
  nfSetId:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSetId'
  rcvRequestCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  sentRequestCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  successfulResponseCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  failureResponseCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  failureCauseStats:
    type: array
    items:
      $ref: '#/components/schemas/FailureCauseOccurrence'
    minItems: 1
  scpFailureCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  scpFailureCauseStats:
    type: array
    items:
      $ref: '#/components/schemas/FailureCauseOccurrence'
    minItems: 1
  reselectionCount:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  reselectionStatList:
    type: array
    items:
      $ref: '#/components/schemas/ReselectionStat'
    minItems: 1
  connectionStatus:
    $ref: '#/components/schemas/ConnectionStatus'
  avgResponseTimeToNF:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
  overloadControlInfo:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/OverloadControlInfo'

```

```

ReselectionStat:
description: The number of times that a reselection happened due to a particular reason
type: object
properties:
  reselectionReason:
    $ref: '#/components/schemas/ReselectionReason'
  count:
    $ref: 'TS29571_CommonData.yaml#/components/schemas/UInteger'
required:
- reselectionReason
- count

```

```

#
# ENUMERATIONS
#

```

```

FailureCause:

```

description: Describes the reasons for failed responses related to SCP egress interface  
anyOf:  
- type: string  
enum:  
- TIME\_OUT  
- SERVER\_ERROR  
- CLIENT\_ERROR  
- OTHER\_FAILURE\_REASONS  
- type: string

ScpEventType:  
description: Describes the supported event types of Nscp\_EventExposure Service  
anyOf:  
- type: string  
enum:  
- SERVICE\_SIGNALLING\_CHARACTERISTICS  
- type: string

ReselectionReason:  
description: Describes the reasons for SCP reselection  
anyOf:  
- type: string  
enum:  
- TARGET\_NF\_UNREACHABLE  
- LOAD\_BASED\_RESELECTION  
- SERVICE\_INSTANCE\_FAILURE  
- UNSPECIFIED  
- type: string

ConnectionStatus:  
description: Describes the connection status  
anyOf:  
- type: string  
enum:  
- ACTIVE  
- INACTIVE  
- type: string

## Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2025-02	CT4#127	C4-250147				Rel-19 Skeleton of new TS on Service Communication Proxy (SCP) Services	0.1.0
2025-02	CT4#127	C4-250148				Rel-19 Abbreviations clause of new TS on Service Communication Proxy (SCP) Services	0.1.0
2025-02	CT4#127	C4-250418				Rel-19 Overview for the SCP service	0.1.0
2025-02	CT4#127	C4-250419				Rel-19 PCR on Services offered by the SCP	0.1.0
2025-02	CT4#127	C4-250640				Rel-19 PCR on API Definition of new SCP Service	0.1.0
2025-04	CT4#128	C4-251129				Pseudo-CR on correction of definition and abbreviation clauses	0.2.0
2025-04	CT4#128	C4-251435				Pseudo-CR on event exposure service description	0.2.0
2025-04	CT4#128	C4-251437				Pseudo-CR on removing template guideline texts	0.2.0
2025-04	CT4#128	C4-251499				Pseudo-CR on service data types used in Subscribe service operation	0.2.0
2025-05	CT4#129	C4-252222				Pseudo-CR on corrections in the OpenAPI	0.3.0
2025-05	CT4#129	C4-252297				Pseudo-CR on Restructure ScpEventFilter to Support Multiple Configurations	0.3.0
2025-05	CT4#129	C4-252298				Pseudo-CR on Spec Cleanup: Template Text Removal and Event Name Correction	0.3.0
2025-06	CT#108	CP-251040				TS presented for information	1.0.0
2025-08	CT4#130	C4-253495				Pseudo-CR on Corrections to SCP Event Exposure Data Definitions, API Versioning, and OpenAPI	1.1.0
2025-08	CT4#130	C4-253517				Pseudo-CR on SCP Event Exposure Data Types and Alignment with SA2 Requirements	1.1.0
2025-09	CT#109	CP-252184				TS presented for approval	2.0.0
2025-09	CT#109					Approved in TSG CT#109	19.0.0
2025-12	CT#110	CP-253150	0001		F	Correction of OpenAPI	19.1.0
2025-12	CT#110	CP-253152	0002	2	F	Correction to data type	19.1.0
2025-12	CT#110	CP-253183	0003	3	F	Correction of SCP event report	19.1.0
2025-12	CT#110	CP-253150	0004		F	Alignment of event name with stage-2	19.1.0
2025-12	CT#110	CP-253150	0005		F	Clarification on expiry time handling during subscription modification	19.1.0
2025-12	CT#110	CP-253150	0006	1	F	Correction of Report Type and clarification of reporting scope	19.1.0
2025-12	CT#110	CP-253167	0009		F	API version and External doc update	19.1.0
2026-03	CT#111	CP-260029	0010		F	Correction of api name	19.2.0
2026-03	CT#111	CP-260029	0011	1	F	Correction of modification of a subscription	19.2.0
2026-03	CT#111	CP-260040	0013		F	API version and External doc update	19.2.0

---

## History

<b>Version</b>	<b>Date</b>	<b>Status</b>
V19.0.0	January 2026	Publication
V19.1.0	February 2026	Publication
V19.2.0	March 2026	Publication