ETSI TS 129 536 V17.4.0 (2024-01)

5G;
5G System;
Network Slice Admission Control Services;
Stage 3
(3GPP TS 29.536 version 17.4.0 Release 17)

Reference
RTS/TSGC-0429536vh40

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 under https://webapp.etsi.org/key/queryform.asp.

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

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

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 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[12] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[13] IETF RFC 7807: "Problem Details for HTTP APIs".

[14] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".[15] 3GPP TS 29.518: "5G System; Access and Mobility Management Service; Stage 3".

[16] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

[17] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

3 Definitions, 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 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].

AF	Application Function
5GC	5G Core Network
AMF	Access Management Function
EAC	Early Admission Control
MCX	Mission Critical Service
MPS	Multimedia Priority Service
NEF	Network Exposure Function
NSAC	Network Slice Admission Control
NSACF	Network Slice Admission Control Function
SMF	Session Management Function

4 Overview

4.1 General

Within the 5GC, the NSACF offers services to the AMF, SMF (or combined SMF+PGW-C), NWDAF and NEF via the Nnsacf service based interface (see 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]).

Figures 4.1 provides the reference model (in service based interface representation and in reference point representation), with focus on the NSACF and the scope of the present specification.

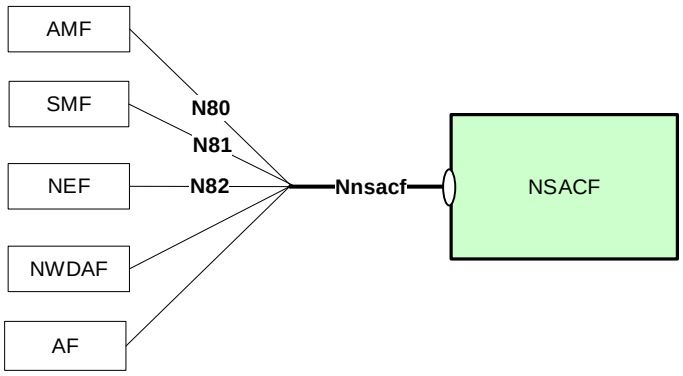

Figure 4-1: Reference model – NSACF

The functionalities supported by the NSACF are listed in clause 6.2.28 of 3GPP TS 23.501 [2].

The services and service operations provided by the Nnsacf interface are listed in clause 5.2.21 of 3GPP TS 23.502 [3].

When the UE connects to EPS and EPS counting is required, it is the combined SMF+PGW-C invokes NSACF services to perform network slice admission control, during PDN connection establishment procedure and PDN connection release procedure, as specified in clause 5.15.11.5 of 3GPP TS 23.501 [2].

NOTE: A trusted AF can access NSACF services either via NEF to NSACF or directly to NSACF. An untrusted AF shall only be allowed to access NSACF services via NEF. If multiple NSACFs are deployed in the network and the trusted AF is interested in the aggregated report, then the trusted AF collects the report from NEF, instead of contacting multiple NSACFs directly.

4.2 NSAC support in roaming

In the roaming scenario, depending on operator's policy and roaming agreement, the NSAC procedure may be performed by the VPLMN for roaming UEs (see clause 5.15.11.3 of 3GPP TS 23.501 [2]).

For roaming UEs with LBO PDU session, the vNSACF offers service to the NF in the VPLMN (e.g. AMF in the VPLMN, anchor SMF in the VPLMN). The hNSACF in the HPLMN is not used in this release of the specification (see clause 4.2.4 of 3GPP TS 23.501 [2]).

If the VPLMN is configured to perform NSAC procedure, for roaming UE with HR PDU session, the vNSACF offers service to the NF in VPLMN (e.g. AMF in VPLMN) while the hNSACF offers service to the NF in HPLMN (e.g. anchor SMF in the HPLMN).

If the NSAC service is only provisioned in the HPLMN and the VPLMN supports NSAC procedure towards the HPLMN for roaming UE with HR PDU session, the hNSACF offers service to both NF in VPLMN and NF in HPLMN (e.g. AMF in VPLMN, anchor SMF in HPLMN).

5 Services offered by the NSACF

5.1 Introduction

The NSACF supports the following services.

Table 5.1-1: NF Services provided by NSACF

Service Name	Description	Example Consumer
Nnsacf_NSAC	This service allows NF service consumer (e.g. AMF) to request NSACF to perform per slice admission control for the number of UEs / PDU sessions.	AMF, SMF
Nnsacf_SliceEventExposure	This service provide event based notifications to the NF service consumer related to the number of UEs registered to a network slice or the number of PDU Sessions established to a network slice.	NEF, AF, NWDAF

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
Nnsacf_NSAC	6.1	per slice admission control service to control the number of UEs / PDU sessions	TS29536_Nnsacf_NSAC.yaml	nnsacf-nsac	A.2
Nnsacf_SliceEvent Exposure	6.2	Slice related event subscription and notification	TS29536_Nnsacf_SliceEventExposure.yaml	nnsacf-slice-ee	A.3

5.2 Nnsacf_NSAC Service

5.2.1 Service Description

The Nnsacf_NSAC service provides the service capability for the NF Service Consumer (e.g. AMF, SMF) to request admission control for UEs accessing a specific network slice, or for PDU sessions to be established to a specific network slice. The following are the key functionalities of this NF service:

- Request the NSACF to control the number of UEs registered to a specific network slice, e.g. perform availability check and update the number of UEs registered to a specific network slice;
- Request the NSACF to control the number of PDU session established to a specific network slice, e.g. perform availability check and update the number of PDU sessions established to a specific network slice;
- Notify the NF Service Consumer (e.g. AMF) of the activation/deactivation of EAC (Early Admission Control) mode for NSAC procedure;

The Nnsacf_NSAC service supports the following service operations.

Table 5.2.1-1: Service operations supported by the Nnsacf_NSAC service

Service Operations	Description	Operation Semantics	Example Consumer(s)
NumOfUEsUpdate	Request the NSACF to perform admission control to control the number of UEs registered to a network slice.	Request/Response	AMF, combined SMF+PGW-C
NumOfPDUsUpdate	Request the NSACF to perform admission control to control the number of PDU sessions established to a network slice.	Request/Response	SMF, combined SMF+PGW-C
EACNotify	Notify the NF Service Consumer of the activation/deactivation of EAC mode.	Subscribe/Notify	AMF

When the UE connects to EPS and EPS counting is required for the S-NSSAI, the combined SMF+PGW-C shall invoke the NumOfUEsUpdate and NumOfPDUsUpdate service operations in sequence. If the NumOfUEsUpdate returns failure, the combined SMF+PGW-C shall not continue invoking the NumOfPDUsUpdate. If the NumOfPDUsUpate returns failure then the combined SMF+PGW-C shall invoke the NumOfUEUpdate to decrease the UE count.

5.2.2 Service Operations

5.2.2.1 Introduction

This clause introduces the related procedures using Nnsacf_NSAC service operations to request the NSACF to control the number of UEs registered to a specific network slice.

5.2.2.2 NumOfUEsUpdate

5.2.2.2.1 General

The NumOfUEsUpdate service operation shall be used by the NF Service Consumer (e.g. AMF, or combined SMF+PGW-C) to request the NSACF to control the number of UEs registered to a specific network slice, e.g. perform availability check and update the number of UEs registered to a network slice. It is used in the following procedures:

- AMF initiated network slice admission control procedure related to control the number of UEs registered to a network slice (see clause 4.2.11.2 of 3GPP TS 23.502 [3]).
- Combined SMF+PGW-C initiated network slice admission control procedure related to control the number of UEs registered to a network slice, in the case of EPS interworking (see clause 5.15.11.5 of 3GPP TS 23.501 [2]).

The operation may also be used to update the number of existing registered UEs in the NSACF when NSAC is enabled or disabled for a slice which is already live in the network.

5.2.2.2.2 Network slice admission control for controlling the number of UEs

The NF Service Consumer (e.g. AMF, combined SMF+PGW-C) shall invoke the NumOfUEsUpdate service operation to request the NSACF to perform network slice admission control procedure related to the number of UEs, by using the HTTP POST method as shown in Figure 5.2.2.2.2-1.

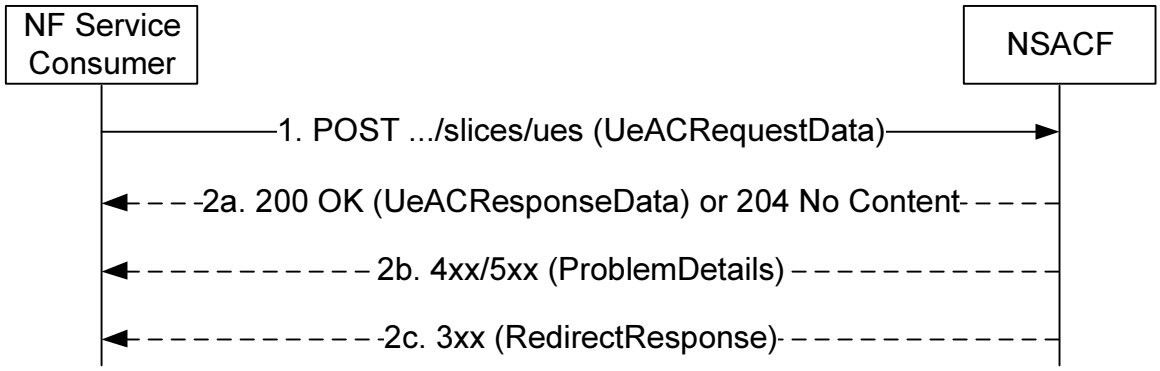

Figure 5.2.2.2.2-1: NSAC procedure for controlling the number of UEs

1. The NF Service Consumer (e.g. AMF, combined SMF+PGW-C) shall send a POST request to the resource representing the network slice admission control related to the number of UEs (i.e. …/slices/ues) in the NSACF.

   The payload body of the POST request shall contain the input data structure (i.e. UeACRequestData) for network slice admission control, which shall contain the following information:

   - the SUPI(s) of the UE(s);
   - the access type, over which the UE registers to the network or deregisters from the network;
   - a list of S-NSSAIs which are subject to NSAC, and for each S-NSSAI an update flag indicates the operation to that S-NSSAI;
   - the NF Instance ID, identifying the requester NF.

   In addition, the POST request may also contain:

   - the EAC notification callback URI. The AMF may provide the EAC notification callback URI at the first interaction with the NSACF, or may provide an updated one in later interactions when it changes. If the EAC notification callback URI is set to null value by the AMF in later interactions, it means the AMF unsubscribes the EAC notification from the NSACF;
   - the additional access type, if the UE deregisters from the network over both 3GPP access and Non-3GPP access.

   The update flag shall be set to "INCREASE" for a UE to be registered to a specific slice, and shall be set to "DECREASE" for a UE to be deregistered from a specific slice.

   For NSAC of roaming UEs, the NF Service Consumer (e.g. AMF) shall provide the S-NSSAI in serving PLMN, and the corresponding mapped S-NSSAI in home PLMN to the NSACF in serving PLMN.

NOTE 1: When multiple S-NSSAIs are supported by a NSACF and multiple S-NSSAIs are required for NSAC for a given UE where EAC mode is active for at least one S-NSSAI, how the AMF triggers NSAC procedure to this NSACF is implementation specific, e.g. the AMF triggers NSAC procedure for all these supported S-NSSAIs before the Registration Accept message or the UE Configuration Update message.

2a. For each S-NSSAI included in UeACRequestData, the NSACF shall perform the following actions:

   - if the update flag is set to "INCREASE", the NSACF shall check whether the UE is already in the UE registration list stored in the NSACF and whether the total number of UEs to this slice will exceed the maximum number of UEs allowed to be registered to this slice:

- if the UE ID is already recorded in the UE registration list but the requester NF is not recorded in the UE registration list, the NSACF shall create a new entry for the UE registration associated with the requester NF and shall also maintain the existing UE registration entries. The total number of UEs registered to this slice is not updated;

- if the UE ID is not recorded in the UE registration list and the total number of UEs (including the UEs indicated in the request and the UEs already stored in the NSACF) does not exceed the maximum number of UEs allowed to be registered to this slice, the NSACF records the indicated UEs to the UE registration list stored in the NSACF, and updates the total number of UEs registered to this slice accordingly;

- if the UE ID is not recorded in the UE registration list and if the total number of UEs will exceed the maximum number of UEs allowed to be registered to this slice, the NSACF shall not record the UE into the UE registration list stored in the NSACF, and shall not update the total number of UEs. Instead, the NSACF shall record this S-NSSAI in the failed list of S-NSSAI in the response message, together with an appropriate value of AcuFailureReason (e.g. "EXCEED_MAX_UE_NUM" as specified in clause 6.1.6.3.5);

- if the update flag is set to "DECREASE" and if the UE is recorded in the UE registration list, the NSACF shall remove the indicated UEs from the UE registration list stored in the NSACF. If there are two or more UE registration entries associated with the UE ID, the NSACF shall only remove the entry associated with the requester NF. After removal, if a UE is no longer recorded in the UE registration list, the NSACF shall decrease the total number of UEs registered to this slice.

- If the update flag is set to "DECREASE" and if the UE is not recorded in the UE registration list, the NSACF shall not decrease the total number of UEs registered to this slice and shall return successful handling for this UE registration.

The NSACF may be configured to perform per access type network slice admission control. In this case, the NSACF shall check whether the access type provided by the NF Service Consumer is configured for NSAC for the indicated S-NSSAI to control the number of UEs. If the access type is not configured for NSAC for the indicated S-NSSAI, the NSACF shall skip the above handling for increasing/decreasing the number of UEs and return successful for this S-NSSAI. If the access type is configured for NSAC for the indicated S-NSSAI, the NSACF shall perform the above handling taking the access type into account and record/remove the UE registration associated with the access type. If the total number of UEs will exceed the maximum number of UEs allowed to be registered to this slice, the NSACF shall record this S-NSSAI in the failed list of S-NSSAI in the response message, together with an appropriate value of AcuFailureReason (e.g. "EXCEED_MAX_UE_NUM" as specified in clause 6.1.6.3.5).

If the NSACF is not configured to perform per access type network slice admission control, the NSACF may perform network slice admission control without taking access type into account. For example, the NSACF is configured with a total quota for the PLMN, but the network slice admission control is not specific to one access type. The NSACF shall record the access type(s) associated with the UE registration. The NSACF shall remove the corresponding UE registration entry when the UE deregisters from all access types.

NOTE 2: For each S-NSSAI that is applicable for NSAC, the NSACF is configured with a total quota for the PLMN. However, the network slice admission control may be configured to apply for one specific access type or both access types.

If in above NSACF handling not all S-NSSAIs are successful, "200 OK" shall be returned, with necessary response data indicating the failed S-NSSAI and the failure reason, e.g. "EXCEED_MAX_UE_NUM".

If in above NSACF handling all S-NSSAIs are successful, "204 No Content" shall be returned which could represent the maximum number of UEs for the S-NSSAI not reached.

NOTE 3: If the PLMN has multiple service areas and there are multiple NSACFs deployed for the network slice, each NSACF may be configured with the maximum number of UEs of the network slice within its service area, e.g. as per operator policy. How to split or synchronize the threshold in multiple NSACFs is left to implementation. Whether and how to guarantee session continuity when a UE moves to new service area with a different NSACF are left to implementation.

NOTE 4: If the NF Service Consumer is AMF, the NSACF may subscribe to AMF Status Change Notifications (e.g. AMF unavailability) via the NRF and update the NF ID accordingly, as described in clause 4.2.11.2 of 3GPP TS 23.502 [3].

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") indicating the error shall be returned.

A ProblemDetails IE shall be included in the payload body of POST response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.1.3.2.3.1-1.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of POST response.

When the procedure is used to perform admission control for a number of UEs, when e.g. NSAC is enabled or disabled for an already live slice, then based on operator policy AMF may allow or disallow sessions for which NSACF returned a reject.

5.2.2.3 EACNotify

5.2.2.3.1 General

The EACNotify service operation shall be used by the NSACF to inform the NF Service Consumer (e.g. AMF) of the activation/deactivation of EAC mode. It is used in the following procedures:

- NSACF initiated configuration on EAC mode procedure (see clause 4.2.11.3 of 3GPP TS 23.502 [3]).

5.2.2.3.2 NSACF initiated EAC mode configuration

The EACNotify service operation shall be used by the NSACF to configure the EAC mode(s) for S-NSSAI(s) to the NF Service Consumer (e.g. AMF). The EACNotify service operation shall be triggered when the NSACF decides to set the EAC mode for an S-NSSAI to "ACTIVE" if the number of UEs registered to an S-NSSAI is above certain threshold, or set the EAC mode for an S-NSSAI to "DEACTIVE" if the number of UEs registered to an S-NSSAI is below certain threshold. The activation threshold and the deactivation threshold may be same or different.

If NF Service Consumer has implicitly subscribed to receive EAC notification, the NSACF shall notify the NF Service Consumer (e.g. AMF) to configure the EAC mode by using the HTTP POST method as shown in Figure 5.2.2.2.3-1.

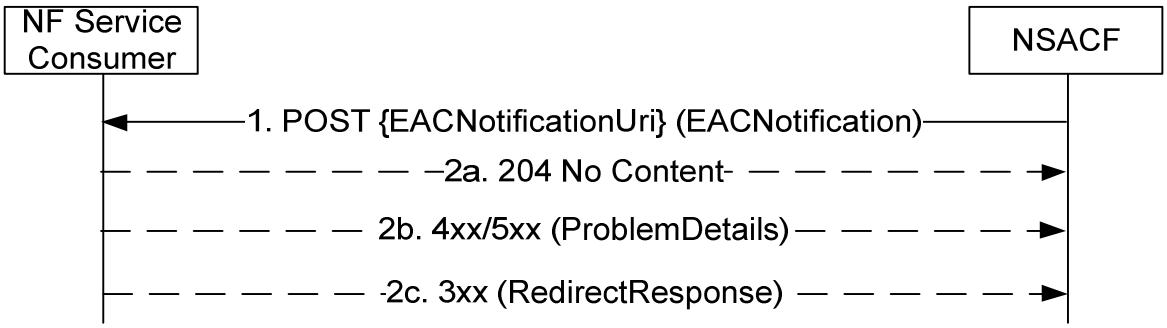

Figure 5.2.2.2.3-1: NSACF initiated EAC mode configuration procedure

1. The NSACF shall send a POST request to the EAC Notification callback URI provided by the NF Service Consumer (e.g. AMF).

   The payload body of the POST request shall contain the notification payload (i.e. EACNotification), which shall contain the following information:

   - S-NSSAI(s);
   - the EAC mode for each S-NSSAI.

   The callback URI may be provided by the AMF in the first interaction with the NSACF, or in later interactions when the callback URI is changed.

2a. On success, "204 No Content" shall be returned and the payload body of the POST response shall be empty.

2b. On failure, one of the HTTP status code listed in Table 6.1.5.2.3.1-2 shall be returned. For a 4xx/5xx response, the message body shall contain a ProblemDetails structure with the "cause" attribute set to one of the application error listed in Table 6.1.7.3-1.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of POST response.

The NSACF may try several times to send EAC notification to the AMF, if no response is received from the AMF e.g. AMF is out of service. If the subsequent try still fails, the NSACF should stop sending EAC notification, unless the AMF becomes available.

5.2.2.4 NumOfPDUsUpdate

5.2.2.4.1 General

The NumOfPDUsUpdate service operation shall be used by the NF Service Consumer (e.g. SMF) to request the NSACF to control the number of PDU sessions registered to a specific slice, e.g. perform availability check and update the number of PDU sessions registered to a slice. It is used in the following procedures:

- SMF initiated network slice admission control procedure for controlling the number of PDU sessions registered to a network slice (see clause 4.2.11.4 of 3GPP TS 23.502 [3]).

- Combined SMF+PGW-C initiated network slice admission control procedure for controlling the number of PDU sessions registered to a network slice, in the case of EPS interworking (see clause 5.15.11.5 of 3GPP TS 23.501 [2], and clause 4.2.11.4 of 3GPP TS 23.502 [3]).

  The operation may also be used to update the number of existing PDU Sessions in the NSACF when NSAC is enabled or disabled for a slice which is already live in the network.

5.2.2.4.2 Network slice admission control for controlling the number of PDU sessions

The NF Service Consumer (e.g. SMF, combined SMF+PGW-C) shall invoke the NumOfPDUsUpdate service operation to request the NSACF to perform network slice admission control procedure related to the number of PDU sessions, by using the HTTP POST method as shown in Figure 5.2.2.4.2-1.

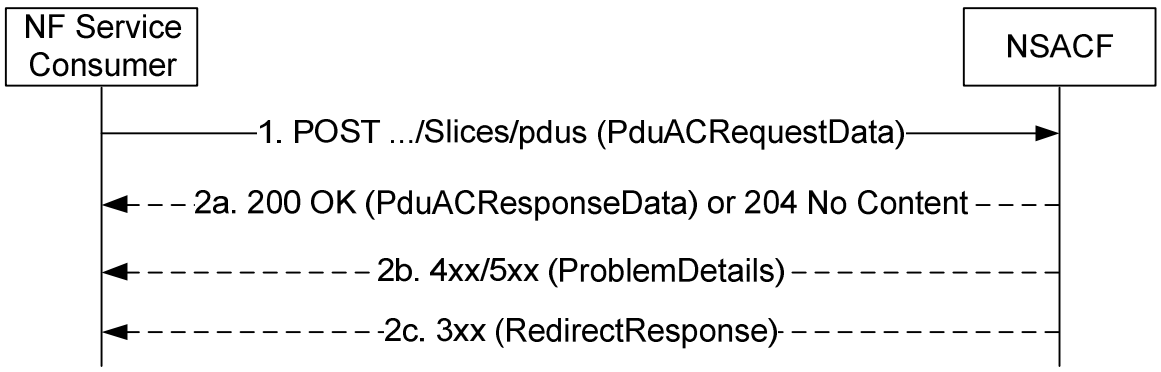

Figure 5.2.2.4.2-1: NSAC procedure for controlling the number of PDU sessions

1. The NF Service Consumer (e.g. SMF) shall send a POST request to the resource representing the network slice admission control related to the number of PDU sessions (i.e. …/slices/pdus) in the NSACF.

   The payload body of the POST request shall contain the input data structure (i.e. PduACRequestData) for network slice admission control, which shall contain the following information:

   - the SUPI of the UE;

   - the access type, over which the PDU session is to be established or released;

- the PDU session ID(s);
- a list of S-NSSAIs which are subject to NSAC, and for each S-NSSAI an update flag indicates the operation to that S-NSSAI.

In addition, the POST request may also contain:

- the NF Instance ID of the requester NF (i.e. SMF);
- the PGW-C FQDN, if the request is sent by a combined SMF+PGW-C in EPS interworking case.
- the additional access type, for an Multi-Access PDU session, if the PDU session is to be established over both 3GPP access and Non-3GPP access, or if the PDU session is to be released from both 3GPP access and Non-3GPP access.

The update flag within the PduACRequestData shall be set to the value as following:

- "INCREASE" for a Single-Access PDU session which is to be established, or for an Multi-Access PDU session when new access leg(s) is to be established;
- "DECREASE" for a Single-Access PDU session which is to be released, or for an Multi-Access PDU session when existing access leg(s) is to be removed;
- "UPDATE" for a Single-Access PDU session when the access type is to be replaced with a new access type during inter access mobility.

  For LBO cases, the NF Service Consumer in serving PLMN (e.g. vSMF) shall provide the S-NSSAI in serving PLMN, and the corresponding mapped S-NSSAI in home PLMN to the NSACF in serving PLMN. For PDU sessions in the home-routed roaming case, the NF Service Consumer in home PLMN (e.g. hSMF) shall provide S-NSSAI(s) in home PLMN to the NSACF in the home PLMN.

2a. For each S-NSSAI included in PduACRequestData, the NSACF shall perform the following actions:

- if the update flag is set to "INCREASE", the NSACF shall check whether the PDU session is already recorded in the PDU registration list in the NSACF and whether the total number of PDU sessions to this slice will exceed the maximum number of PDU sessions allowed to be registered to this slice:
  - if the PDU session (identified by the UE ID and the PDU session ID) is already recorded in the PDU registration list, the NSACF shall skip recording this PDU session and shall not increase the total number of PDU sessions established to this network slice;
  - if the PDU session is not recorded in the PDU registration list and the total number of PDU sessions (including the PDU session indicated in the request and the PDU sessions already stored in the NSACF) does not exceed the maximum number of PDU sessions allowed to be registered to this slice, the NSACF records the PDU session to the PDU registration list stored in the NSACF, and updates the total number of PDU sessions registered to this slice accordingly;
  - if the PDU session is not recorded in the PDU registration list and if the total number of PDU sessions will exceed the maximum number of PDU sessions allowed to be registered to this slice, the NSACF shall not record the PDU session into the PDU registration list stored in the NSACF, and shall not update the total number of PDU sessions. Instead, the NSACF shall record this S-NSSAI in the failed list of S-NSSAI in the response message, together with an appropriate value of AcuFailureReason (e.g. "EXCEED_MAX_PDU_NUM" as specified in clause 6.1.6.3.5);
- if the update flag is set to "DECREASE" and if the PDU session is recorded in the PDU registration list, the NSACF decreases the total number of PDU sessions registered to this slice, and removes the indicated PDU session from the PDU registration list stored in the NSACF.
- If the update flag is set to "DECREASE" and if the PDU session is not recorded in the PDU registration list, the NSACF shall not decrease the total number of PDU sessions registered to this slice and shall return successful handling for this PDU registration.
- If the update flag is set to "UPDATE", the NSACF shall locate the existing entry in the PDU registration list and update the access type associated to the PDU session to which indicated in the request message.

The NSACF may be configured to perform per access type network slice admission control. In this case, the NSACF shall check whether the access type provided by the NF Service Consumer is configured for NSAC for the indicated S-NSSAI to control the number of PDU sessions. If the access type is not configured for NSAC for the indicated S-NSSAI, the NSACF shall skip the above handling for increasing/decreasing the number of PDU sessions and shall return successful for this S-NSSAI. If the access type is configured for NSAC for the indicated S-NSSAI, the NSACF shall perform the above handling taking the access type into account. If the update flag is set to "UPDATE", the NSACF shall first increase the number of PDU sessions for the new access type, and if successful then decrease the number of PDU sessions for the old access type. If the total number of PDU sessions will exceed the maximum number of PDU sessions allowed to be registered to this slice, the AcuFailureReason shall indicate the applied access type (e.g. "EXCEED_MAX_PDU_NUM_3GPP" or "EXCEED_MAX_PDU_NUM_N3GPP" as specified in clause 6.1.6.3.5).

If the NSACF is not configured to perform per access type network slice admission control, the NSACF may perform network slice admission control without taking access type into account. For example, the NSACF is configured with a total quota for the PLMN, but the network slice admission control is not specific to one access type. The NSACF shall record the access type(s) associated with the PDU registration. The NSACF shall remove the PDU registration entry when the PDU session is released from all access types.

NOTE 1: For each S-NSSAI that is applicable for NSAC, the NSACF is configured with a total quota for the PLMN. However, the network slice admission control may be configured to apply for one specific access type or both access types.

If in above NSACF handling not all S-NSSAIs are successful, "200 OK" shall be returned, with necessary response data, e.g. indicating the failed S-NSSAI(s).

If in above NSACF handling all S-NSSAIS are successful, "204 No Content" shall be returned.

NOTE 2: If the PLMN has multiple service areas and there are multiple NSACFs deployed for the network slice, each NSACF may be configured with the maximum number of PDU Sessions of the network slice within its service area, e.g. as per operator policy. How to split or synchronize the threshold in multiple NSACFs is left to implementation. Whether and how to guarantee session continuity when a UE moves to new service area with a different NSACF are left to implementation.

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") indicating the error shall be returned.

A ProblemDetails IE shall be included in the payload body of POST response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.1.3.3.3.1-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse shall be included in the payload body of POST response.

When the procedure is used to perform admission control for a number of UEs, when e.g. NSAC is enabled or disabled for an already live slice, then based on operator policy, SMF may allow or disallow sessions for which NSACF returned a reject.

5.3 Nnsacf_SliceEventExposure Service

5.3.1 Service Description

The Nnsacf_SliceEventExposure services provide event based notifications to the consumer NF (e.g. to AF via NEF) related to the number of UEs registered to a network slice or the number of PDU Sessions established to a network slice.

If, in accordance with operator policy and national/regional regulations, the NF Service Consumer (i.e. the AMF or the SMF) needs to exempt UEs/PDU Sessions that are used for emergency, mission critical and/or priority services (e.g. MCS, MPS) from NSAC, then the NF service consumer may send a request to NSACF and ignore the NSACF response. Therefore, if a UE/PDU session is rejected by NSACF, then the reports generated by the NSACF would not have counts of those UEs/PDU-Sessions, despite the UEs accessing the corresponding slice(s). Alternatively, the NF Service Consumer (i.e. the AMF or the SMF) may not invoke the corresponding NSAC procedure for the exempted

UE/PDU Session, i.e. those UEs/PDU Sessions are not counted towards the maximum number of UEs/PDU Sessions (see clause 5.15.11.0 of 3GPP TS 23.501 [2]).

5.3.2 Service Operations

5.3.2.1 Introduction

For the Nnsacf_SliceEventExposure service the following service operations are defined:

- Subscribe, including creation or modification of a subscription;
- Unsubscribe;
- Notify.

5.3.2.2 Subscribe

5.3.2.2.1 General

This service operation is used by the consumer NF (e.g. NEF, AF or NWDAF) to subscribe or modify a subscription with the NSACF for event based notifications of the number of UEs registered to a network slice or the number of PDU Sessions established to a network slice.

5.3.2.2.2 Creation of a subscription

The Subscribe service operation is invoked by a NF Service Consumer (e.g. NEF, AF or NWDAF) towards the NSACF, when it needs to create a subscription to monitor the event relevant to the NSACF.

The NF Service Consumer shall request to create a new subscription by using HTTP method POST with URI of the subscriptions collection, see clause 6.2.3.1.

The NF Service Consumer shall include the following information in the HTTP message body:

- NF ID, indicates the identity of the network function instance initiating the subscription;
- Notification URI, indicates the address to deliver the event notifications generated by the subscription;
- Notification Correlation ID, indicates the correlation identity to be carried in the event notifications, the value of this IE shall be unique per subscription for a given NF service consumer receiving the notification;
- SAC Event Type, defines whether to notify the number of UEs registered with a network slice or the number of PDU Sessions established on a network slice;
- Event Filter, indicate the S-NSSAI(s) in serving PLMN and/or mapped S-NSSAI(s) in home PLMN to be monitored and reported.
- SAC Event Report Triggers, defines whether the notification is threshold triggered (e.g. the notification is triggered when the current number of UEs or PDU Sessions with a network slice reaches a defined threshold value) or the notification is periodic triggered (e.g. the notification is triggered at expiry of a periodic timer).
- Notification threshold if the SAC Event Report Triggers is threshold triggered, defines a numeric value or a percentage of the maximum number of the UEs or PDU Sessions per network slice;
- Notification periodicity if the SAC Event Report Triggers is periodic triggered, defines the time between the notification periodicity.

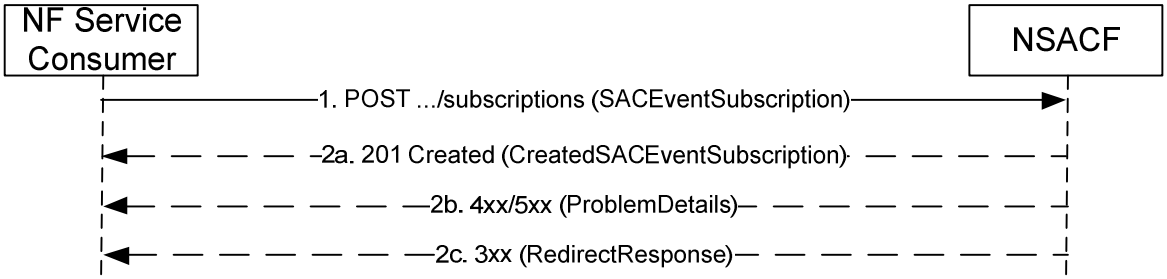

Figure 5.4.2.2.2-1 Subscribe for Creation

1. The NF Service Consumer (e.g. NEF, AF or NWDAF) shall send a POST request to create a subscription resource in the NSACF. The payload body of the POST request shall contain a representation of the individual subscription resource to be created. The request may contain an expiry time, suggested by the NF Service Consumer, representing the time up to which the subscription is desired to be kept active and the time after which the subscribed event(s) shall stop generating report.

2a. On success, the request is accepted, the NSACF shall include a HTTP Location header to provide the location of a newly created resource (subscription) together with the status code 201 indicating the requested resource is created in the response message.

The response, based on operator policy and taking into account the expiry time included in the request, may contain the expiry time, as determined by the NSACF, after which the subscription becomes invalid. Once the subscription expires, if the NF Service Consumer wants to keep receiving notifications, it shall create a new subscription in the NSACF. The NSACF shall not provide the same expiry time for many subscriptions in order to avoid all of them expiring and recreating the subscription at the same time. If the expiry time is not included in the response, the NF Service Consumer shall consider the subscription to be valid without an expiry time.

If the immediateFlag attribute is set to "true" in the request message, the NSACF shall include the current number of UEs or PDU Sessions per network slice in the response immediately.

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") shall be returned.

A ProblemDetails IE shall be included in the payload body of POST response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.2.3.2.3.1-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of POST response.

5.3.2.2.3 Modification of a subscription

The Subscribe service operation is invoked by a NF Service Consumer (e.g. NEF, AF or NWDAF) towards the NSACF, when it needs to modify an existing subscription previously created by itself at the NSACF.

When the subscription is to be expired, the NF service consumer may request the NSACF to update the subscription by indicating a new expiry time. The NSACF may return a new expiry time based on local policy, taking into account of the NF service consumer provided expiry time.

To perform a partial update of the subscription of a given subscription Id, the NF Service Consumer shall issue an HTTP PATCH request, as shown in Figure 5.3.2.2.3-1. This partial update shall be used to add, delete and/or replace individual parameters of the subscription.

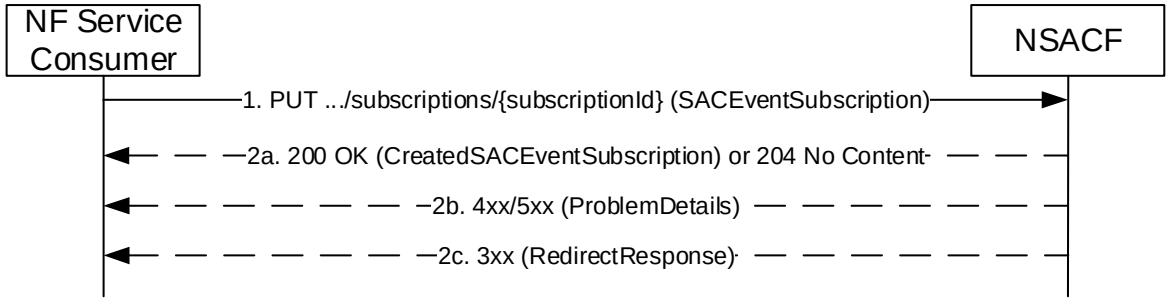

Figure 5.3.2.2.3-1 Subscription partial modification

1. The NF Service Consumer (e.g. NEF, AF or NWDAF) shall send a PATCH request to the resource URI representing the individual subscription, identified by the {subscriptionId}. The payload body of the PATCH request shall contain the list of operations (add/delete/replace) to be applied to parameters in the individual subscription.

2a. On success, the request is accepted, the NSACF shall return the representation of the updated subscription resource with the status code "200 OK", or "204 No Content" shall be returned.

"204 No Content" may be returned, if the NF Service Producer accepts entirely the resource representation provided by the NF Service Consumer in the request. For example, the request contained a proposed expiry time and it is accepted by the NF Service Producer as the expiration time for the subscription, or the request did not contain a proposed expiry time and no expiration time is set by the NF Service Producer for the subscription.

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") shall be returned.

A ProblemDetails IE shall be included in the payload body of PATCH response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.2.3.3.3.1-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of PATCH response.

To perform a complete replacement of the subscription of a given subscription Id, the NF Service Consumer shall issue an HTTP PUT request, as shown in Figure 5.3.2.2.3-2:

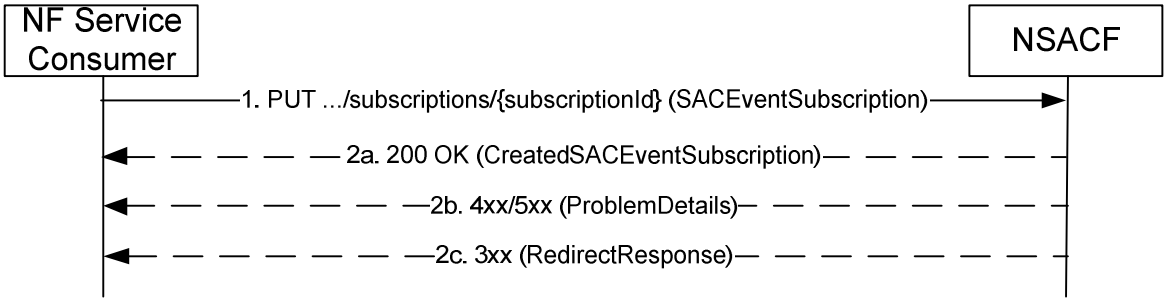

Figure 5.3.2.2.3-2 Subscription Complete Replacement

1. The NF service consumer (e.g. NEF, AF or NWDAF) shall send a PUT request to the resource URI representing the individual subscription, identified by the {subscriptionId}. The payload body of the PUT request shall contain a representation of the individual subscription to be completely replaced in the NSACF.

2a. On success, the request is accepted, the NSACF shall include the resource (subscription) after replacement together with the status code "200 OK" indicating the requested resource is updated in the response message.

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") shall be returned.

A ProblemDetails IE shall be included in the payload body of PUT response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.2.3.3.3.2-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of PUT response.

5.3.2.2.4 Creation of a one time and immediate reporting subscription

The NF Service Consumer (e.g. NEF, AF or NWDAF) may request the NSACF to immediately provide the current network slice status information (e.g. the number of UEs registered to a network slice, the current number of PDU Sessions established to a network slice). In this case, the NF Service Consumer (e.g. NEF, AF or NWDAF) shall request the NSACF to create a temporary subscription and response with immediate report, as follows.

1. The NF Service Consumer shall send a POST request as specified in step 1 of clause 5.3.2.2.2, with the following additional information:

   - the maxReports attribute set to 1 and the immediateFlag attribute set to "true".

2a. The NSACF shall send a POST response as specified in step 2a of clause 5.3.2.2.2, with the following additional information:

   - the NSACF shall include the current number of UEs or PDU Sessions per network slice in the response immediately and shall terminate the subscription of the event.

   The NSACF shall terminate the subscription of the event after sending response to the NF Service Consumer.

2b. Same as step 2b of figure 5.3.2.2.2-1.

2c. Same as step 2c of figure 5.3.2.2.2-1.

5.3.2.3 Unsubscribe

5.3.2.3.1 General

This service operation is used by the consumer NF (e.g. NEF, AF or NWDAF) to unsubscribe from the event notification.

The NF Service Consumer (e.g. NEF, AF or NWDAF) shall unsubscribe to the subscription by using HTTP method DELETE.

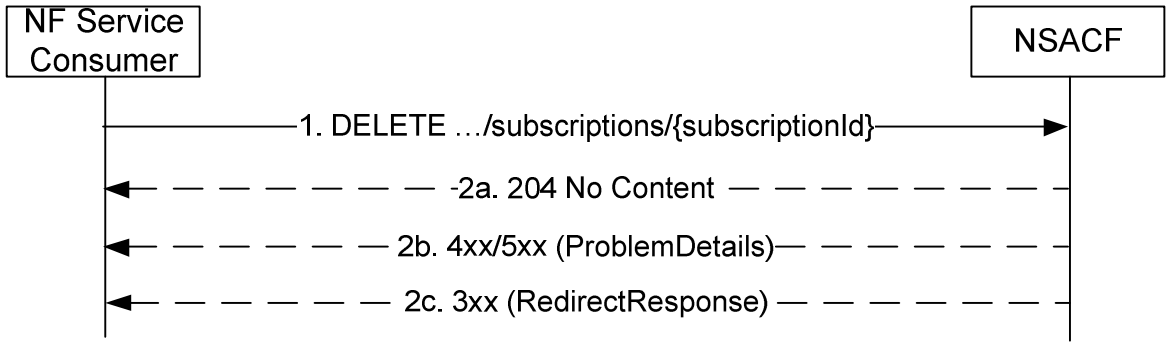

Figure 5.3.2.3.1-1: Unsubscribe a subscription

1. The NF Service Consumer (e.g. NEF, AF or NWDAF) shall send a DELETE request to delete an existing subscription resource in the NSACF.

2a. On success, the request is accepted, the NSACF shall reply with the status code 204 indicating the resource identified by subscription ID is successfully deleted in the response message.

2b. On failure, the appropriate HTTP status code (e.g. "403 Forbidden") shall be returned.

A ProblemDetails IE shall be included in the payload body of DELETE response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.2.3.3.3.3-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of DELETE response.

5.3.2.4 Notify

5.3.2.4.1 General

This service operation is used by the NSACF to report the current number of UEs registered with a network slice or the current number of PDU Sessions established on a network slice in numbers or in percentage from the maximum allowed numbers.

While counting the number of UEs registered to a network slice, the NSACF shall not count twice the UE Ids stored temporarily due to the AMF mobility scenario.

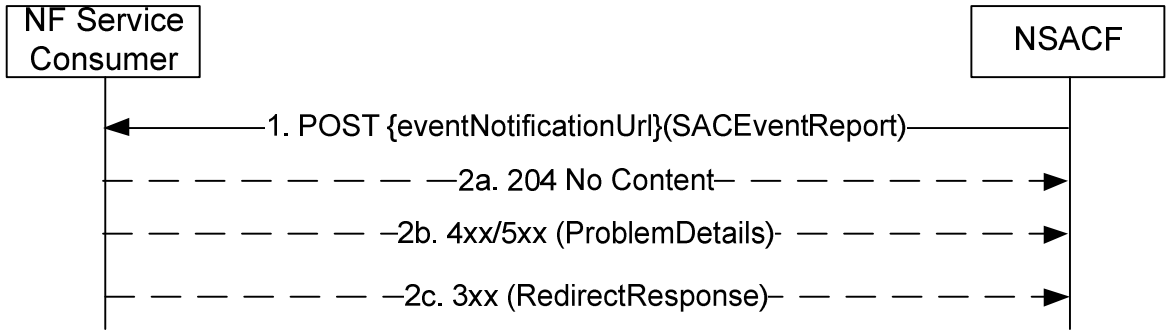

Figure 5.3.2.4.1-1: Notify

1. The NSACF shall send a POST request to send a notification.

   If the notification is threshold triggered, the NSACF shall send the notification every time if there is a change from being below the threshold to reach the threshold, or from reaching the threshold to coming down below the threshold (see clause 4.15.3.2.10 of 3GPP TS 23.502 [3]). When a subscription is created and the current number of UEs or number of PDU sessions reaches the threshold, the NSACF shall send the notification immediately.

EXAMPLE:

If the threshold for the reporting of the number of registered UEs is 100, the behaviour of the NSACF as below:

- the current number of registered UEs is 100 when the subscription is created, the NSACF shall send a notification to the NF service consumer, then
- the current number of registered UEs is changed to 99, the NSACF shall send a notification to the NF service consumer, then
- the current number of registered UEs is changed to 90, the NSACF shall not send notification, then
- the current number of registered UEs is changed to 100, the NSACF shall send a notification to the NF service consumer, then
- the current number of registered UEs is changed to 110, the NSACF shall not send notification.

For periodic reporting, the NSACF shall contain the current number of registered UEs in the concerned network slice or the current number of established PDU sessions in the concerned network slice expressed in percentage and in numerical to the NF Service Consumer.

2a. On success, "204 No content" shall be returned by the NF Service Consumer (e.g. NEF, AF or NWDAF).

2b. On failure, the appropriate HTTP status code (e.g. "307 Temporary Redirect") shall be returned and appropriate additional information should be returned.

A ProblemDetails IE shall be included in the payload body of POST response, with the "cause" attribute of ProblemDetails set to application error codes specified in table 6.2.5.2.2.1-3.

2c. On redirection, "307 Temporary Redirect" or "308 Permanent Redirect" shall be returned. A RedirectResponse IE shall be included in the payload body of POST response.

6 API Definitions

6.1 Nnsacf_NSAC Service API

6.1.1 Introduction

The Nnsacf_NSAC shall use the Nnsacf_NSAC API.

The API URI of the Nnsacf_NSAC 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 "nnsacf-nsac".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 5.3.

6.1.2 Usage of HTTP

6.1.2.1 General

HTTP/2, IETF RFC 7540 [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 Nnsacf_NSAC 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 7807 [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

The figure 6.1.3.1-1 describes the resource URI structure of the Nnsacf-NSAC API.

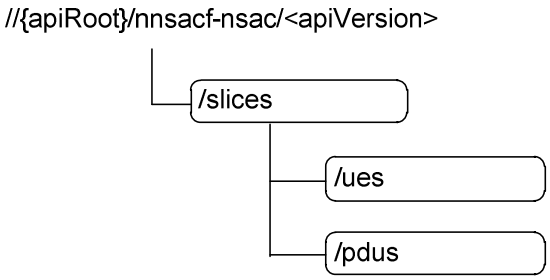

Figure 6.1.3.1-1: Resource URI structure of the Nnsacf_NSAC API

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 name	Resource URI	HTTP method or custom operation	Description
Slice Collection Subject to NSAC for UEs (Collection)	/slices/ues	POST	Request the NSACF to perform network slice admission control related to the number of UEs registered to a network slice, or a group of network slices.
Slice Collection Subject to NSAC for PDU sessions (Collection)	/slices/pdus	POST	Request the NSACF to perform network slice admission control related to the number of PDU sessions established to a network slice, or a group of network slices.

6.1.3.2 Resource: Slice Collection Subject to NSAC for UEs

6.1.3.2.1 Description

This resource represents the collection of slice subject to NSAC for UEs.

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

6.1.3.2.2 Resource Definition

Resource URI: **{apiRoot}/<apiName>/<apiVersion>/slices/ues**

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
apiVersion	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

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
UeACRequestData	M	1	Request data for NSAC procedure related to the number of UEs per slice.

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
UeACResponseData	M	1	200 OK	Response data for NSAC procedure related to the number of UEs per slice, in the case of not all S-NSSAIs are successful in the NSAC procedure.
n/a			204 No Content	Upon success. Indicates all S-NSSAIs are successful in the NSAC procedure.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during a NSAC procedure. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	When used to represent the failure of NSAC procedure, the "cause" attribute of the "ProblemDetails" shall be set to one of the following application error codes: - SLICE_NOT_FOUND, if all S-NSSAIs provided in the request are not found from the NSSAI which are subject to NSAC procedure; - ALL_SLICE_FAILED, if the list of S-NSSAIs is fully failed in the NSAC procedure.
NOTE 1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.2.3.1-4: Headers supported by the 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.2.3.1-5: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.1.3.2.4 Resource Custom Operations

In this release of this specification, no custom operations associated to this resource is defined.

6.1.3.3 Resource: Slice Collection Subject to NSAC for PDU sessions

6.1.3.3.1 Description

This resource represents the collection of slice subject to NSAC for PDU sessions.

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

6.1.3.3.2 Resource Definition

Resource URI: **{apiRoot}/<apiName>/<apiVersion>/slices/pdus**

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
apiVersion	string	See clause 6.1.1

6.1.3.3.3 Resource Standard Methods

6.1.3.3.3.1 POST

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 POST method on this resource

Name	Data type	P	Cardinality	Description	Applicability

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

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

Data type	P	Cardinality	Description
PduACRequestData	M	1	Request data for NSAC procedure related to the number of PDU sessions per slice.

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

Data type	P	Cardinality	Response codes	Description
PduACResponseData	M	1	200 OK	Response data for NSAC procedure related to the number of PDU sessions per slice, in the case of not all S-NSSAIs are successful in the NSAC procedure.
n/a			204 No Content	Upon success. Indicates all S-NSSAIs are successful in the NSAC procedure.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set. (NOTE 2)
ProblemDetails	O	0..1	403 Forbidden	When used to represent the failure of NSAC procedure, the "cause" attribute of the "ProblemDetails" shall be set to one of the following application error codes: - SLICE_NOT_FOUND, if all S-NSSAIs provided in the request are not found from the NSSAI which are subject to NSAC procedure; - ALL_SLICE_FAILED, if the list of S-NSSAIs is fully failed in the NSAC procedure.
NOTE 1: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply. NOTE 2: RedirectResponses may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4].				

Table 6.1.3.3.3.1-4: Headers supported by the 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.1.3.3.3.1-5: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.1.3.3.4 Resource Custom Operations

In this release of this specification, no custom operations associated to this resource is defined.

6.1.4 Custom Operations without associated resources

In this release of this specification, no custom operations without associated resources are defined.

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)
EAC Mode Notification	{EACNotificationUri}	POST	Notify the NF Service Customer (e.g. AMF) of the activation/deactivation of EAC mode.

6.1.5.2 EAC Mode Notification

6.1.5.2.1 Description

The EAC Mode Notification is used by the NSACF to inform the NF Service Consumer (e.g. AMF) of the activation/deactivation of EAC mode.

6.1.5.2.2 Target URI

The Callback URI **"{EACNotificationUri}"** 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
eacNotificationUri	Notification URI for receiving EAC mode notification.

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
EACNotification	M	1	EAC mode notification

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

Data type	P	Cardinality	Response codes	Description
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.				

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 Nnsacf_NSAC service based interface protocol.

Table 6.1.6.1-1: Nnsacf_NSAC specific Data Types

Data type	Clause defined	Description	Applicability
UeACRequestData	6.1.6.2.2	Input data for NSAC procedure related to the number of UEs per slice.	
UeACResponseData	6.1.6.2.3	Response data of NSAC procedure for controlling the number of UEs.	
EACNotification	6.1.6.2.4	EAC mode notification	
AcuOperationItem	6.1.6.2.5	An operation item for NSAC procedure, indicating an S-NSSAI subject to NSAC and the associated operation.	
AcuFailureItem	6.1.6.2.6	A failure item which indicates the failed S-NSSAI and the failure reason.	
PduACRequestData	6.1.6.2.7	Input data for NSAC procedure related to the number of PDUs per slice.	
PduACResponseData	6.1.6.2.8	Response data of NSAC procedure for controlling the number of PDU sessions.	
EACMode	6.1.6.3.3	EAC mode	
AcuFlag	6.1.6.3.4	Update Flag for NSAC procedure	
AcuFailureReason	6.1.6.3.5	Indicates the failure reason for an S-NSSAI in the NSAC procedure	
UeACRequestInfo	6.1.6.2.9	One item of a UE and associated NSAC action.	
PduACRequestInfo	6.1.6.2.10	One item of a PDU session and associated NSAC action.	

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

Table 6.1.6.1-2: Nnsacf_NSAC re-used Data Types

Data type	Reference	Comments	Applicability
ProblemDetails	3GPP TS 29.571 [16]	Problem Details	
RedirectResponse	3GPP TS 29.571 [16]	Redirect Response	
Supi	3GPP TS 29.571 [16]	Subscription Permanent Identifier	
Snssai	3GPP TS 29.571 [16]	Single NSSAI	
NfInstanceId	3GPP TS 29.571 [16]	NF Instance ID	
Uri	3GPP TS 29.571 [16]	Resource or callback URI	
AccessType	3GPP TS 29.571 [16]	Access Type	
NFType	3GPP TS 29.510 [17]	NF Type	
Fqdn	3GPP TS 29.571 [16]	FQDN	
PduSessionId	3GPP TS 29.571 [16]	PDU Session Identifier	
PlmnId	3GPP TS 29.571 [16]	PLMN ID	

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: UeACRequestData

Table 6.1.6.2.2-1: Definition of type UeACRequestData

Attribute name	Data type	P	Cardinality	Description	Applicability
ueACRequestInfo	array(UeACRequestInfo)	M	1..N	List of UEs and their associated NSAC action details	
nfId	NfInstanceId	M	1	Indicates the NF Instance ID. When present, it shall carry one of the following values: - the AMF Instance ID, if the request is from an AMF; - the SMF Instance ID, if the request is from a combined SMF+PGW-C in EPS interworking case.	
nfType	NFType	O	0..1	Indicates the NF type of the requester NF. When present, it shall carry one of the following values: - NFType=AMF, if the request is from an AMF; - NFType=SMF, if the request is from a combined SMF+PGW-C in EPS interworking case.	
eacNotificationUri	Uri	O	0..1	Indicates the EAC notification callback URI. If the EAC notification callback URI is present, the AMF Instance ID shall also be present.	
NOTE: If the NF consumer is combined SMF+PGW-C, the combined SMF+PGW-C determines the Access Type based on the RAT type parameter in the PMIP or GTP message received from the ePDG; or alternatively it can internally determine the Access Type based on the source node (e.g. SGW) sending the request for the PDN Connection establishment.					

6.1.6.2.3 Type: UeACResponseData

Table 6.1.6.2.3-1: Definition of type UeACResponseData

Attribute name	Data type	P	Cardinality	Description	Applicability
acuFailureList	map(array(AcuFailureItem))	C	1..N(1..M)	Indicates a list of S-NSSAI which is failed in the NSAC procedure, and the reasons for each S-NSSAI. Key of the map is the SUPI of the UE.	

6.1.6.2.4 Type: EACNotification

Table 6.1.6.2.4-1: Definition of type EACNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
eacModeList	map(EACMode)	O	1..N	a map of EAC Mode where the S-NSSAI serves as the key.	

6.1.6.2.5 Type: AcuOperationItem

Table 6.1.6.2.5-1: Definition of type AcuOperationItem

Attribute name	Data type	P	Cardinality	Description	Applicability
updateFlag	AcuFlag	M	1	Indicates the operation (i.e. increase or decrease) to the impacted S-NSSAI.	
snssai	Snssai	M	1	Indicates the S-NSSAI for the increase or decrease operation. It shall contain S-NSSAI in serving PLMN or the mapped S-NSSAI in home PLMN.	
plmnId	PlmnId	C	0..1	Indicates the PLMN ID associated to the S-NSSAI for increase or decrease operation. It shall be present in the NSAC procedure for the HR or LBO roaming case, or if the NSACF serves multiple PLMNs.	

6.1.6.2.6 Type: AcuFailureItem

Table 6.1.6.2.6-1: Definition of type AcuFailureItem

Attribute name	Data type	P	Cardinality	Description	Applicability
snssai	Snssai	M	1	Indicates the S-NSSAI which is failed in the NSAC procedure. It shall contain S-NSSAI in serving PLMN or the mapped S-NSSAI in home PLMN.	
reason	AcuFailureReason	M	1	Indicates the reason of an S-NSSAI which is failed in the NSAC procedure.	
pduSessionId	PduSessionId	C	0..1	The PDU session Identifier, shall be present when response is for pduAC.	
plmnId	PlmnId	C	0..1	Indicates the PLMN ID associated to the S-NSSAI which is failed in the NSAC procedure. It shall be present in the NSAC procedure for the HR or LBO roaming case, or if the NSACF serves multiple PLMN.	

6.1.6.2.7 Type: PduACRequestData

Table 6.1.6.2.7-1: Definition of type PduACRequestData

Attribute name	Data type	P	Cardinality	Description	Applicability
pduACRequestInfo	array(PduACRequestInfo)	M	1..N	List of UEs and their associated NSAC action details	
nfId	NfInstanceId	O	0..1	Indicates the SMF Instance ID.	
pgwFqdn	Fqdn	O	0..1	Indicates the PGW-C FQDN, if the request is from a combined SMF+PGW-C, in EPS interworking case.	

6.1.6.2.8 Type: PduACResponseData

Table 6.1.6.2.8-1: Definition of type PduACResponseData

Attribute name	Data type	P	Cardinality	Description	Applicability
acuFailureList	map(array(AcuFailureItem))	C	1..N(1..2)	Indicates a list of S-NSSAIs which are failed in the NSAC procedure, and the reasons for each S-NSSAI. Key of the map is the SUPI of the UE.	

6.1.6.2.9 Type: UeACRequestInfo

Table 6.1.6.2.x-1: Definition of type UeACRequestInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
Supi	Supi	M	1	Supi	
anType	AccessType	M	1	Indicates the access type over which the UE registers to the network or deregisters from the network. (NOTE)	
acuOperationList	array(AcuOperationItem)	M	1..N	A list of S-NSSAI to which the UE is to be registered or from which the UE is to be de-registered.	
additionalAnType	AccessType	O	0..1	Indicates the additional access type, when the UE deregisters from the network, if the UE previously registered to the network over 3GPP access and Non-3GPP access	

6.1.6.2.10 Type: PduACRequestInfo

Table 6.1.6.2.7-1: Definition of type PduACRequestData

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi	M	1	Supi	
anType	AccessType	M	1	Indicates the access type over which the PDU session is to be established or released.	
pduSessionId	PduSessionId	M	1	Indicates the PDU session Identifier. During PDU session establishment or release in 5GC, this IE shall indicate the PDU session ID of the PDU session to be established or to be released; During PDN connection establishment or release in EPC, this IE shall indicate the EPS pre-allocated PDU session ID for the corresponding PDU session in 5GC.	
acuOperationList	array(AcuOperationItem)	M	1..2	A list of S-NSSAI to which the PDU session is to be established or from which the PDU session is to be released.	
additionalAnType	AccessType	O	0..1	Indicates the additional access type, for a Multiple-Access PDU session, if the PDU session is to be established over both 3GPP access and Non-3GPP access, or if the PDU session is to be released from both 3GPP access and Non-3GPP access.	

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

6.1.6.3.3 Enumeration: EACMode

The enumeration EACMode represents the mode of Early Admission Control. It shall comply with the provisions defined in table 6.1.6.3.3-1.

Table 6.1.6.3.3-1: Enumeration EACMode

Enumeration value	Description	Applicability
"ACTIVE"	EAC mode is enabled.	
"DEACTIVE"	EAC mode is disabled.	

6.1.6.3.4 Enumeration: AcuFlag

The enumeration AcuFlag indicates the operation (i.e. increase or decrease) applied to a list of S-NSSAI during the NSAC procedure. It shall comply with the provisions defined in table 6.1.6.3.4-1.

Table 6.1.6.3.4-1: Enumeration AcuFlag

Enumeration value	Description	Applicability
"INCREASE"	Indicates the impacted list of S-NSSAI is to be added to the NSACF for a UE (or a PDU session).	
"DECREASE"	Indicates the impacted list of S-NSSAI is to be removed from the NSACF for a UE (or a PDU session).	
"UPDATE"	Indicates for the impacted S-NSSAIs the access type of a PDU session is to be replaced.	

6.1.6.3.5 Enumeration: AcuFailureReason

The enumerationAcuFailureReason indicates the operation result of the NSAC procedure for an individual S-NSSAI. It shall comply with the provisions defined in table 6.1.6.3.5-1.

Table 6.1.6.3.5-1: Enumeration AcuFailureReason

Enumeration value	Description	Applicability
"SLICE_NOT_FOUND"	Indicates that an S-NSSAI is not found by the NSACF from the list of S-NSSAIs which are subject to NSAC procedure.	
"EXCEED_MAX_UE_NUM"	Indicates for an S-NSSAI the number of UEs has exceeded the configured maximum number of UEs, if network slice admission control is not specific to one access type.	
"EXCEED_MAX_UE_NUM_3GPP"	Indicates for an S-NSSAI the number of UEs has exceeded the configured maximum number of UEs, if network slice admission control is required for 3GPP access. (NOTE)	
"EXCEED_MAX_UE_NUM_N3GPP"	Indicates for an S-NSSAI the number of UEs has exceeded the configured maximum number of UEs, if network slice admission control is required for Non-3GPP access. (NOTE)	
"EXCEED_MAX_PDU_NUM"	Indicates for an S-NSSAI the number of PDU sessions has exceeded the configured maximum number of PDU sessions if network slice admission control is not specific to one access type.	
"EXCEED_MAX_PDU_NUM_3GPP"	Indicates for an S-NSSAI the number of PDU sessions has exceeded the configured maximum number of PDU sessions, if network slice admission control is required for 3GPP access.	
"EXCEED_MAX_PDU_NUM_N3GPP"	Indicates for an S-NSSAI the number of PDU sessions has exceeded the configured maximum number of PDU sessions, if network slice admission control is required for Non-3GPP access.	
NOTE: If this value is returned in the NSAC response message, how the NF service consumer (e.g. AMF) utilizes the access information carried in the AcuFailureReason value is implementation specific.		

6.1.6.4 Data types describing alternative data types or combinations of data types

In this release, no alternative data types or combinations of data types are defined in this specification.

6.1.6.5 Binary data

In this release, no binary data types are defined in this specification.

6.1.7 Error Handling

6.1.7.1 General

For the Nnsacf_NSAC 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 Nnsacf_NSAC API.

6.1.7.2 Protocol Errors

No specific procedures for the Nnsacf_NSAC service are specified.

6.1.7.3 Application Errors

The application errors defined for the Nnsacf_NSAC service are listed in Table 6.1.7.3-1.

Table 6.1.7.3-1: Application errors

Application Error	HTTP status code	Description
SLICE_NOT_FOUND	403 Forbidden	All S-NSSAIs provided in the request are not found by the NSACF from the list of S-NSSAIs which are subjected to NSAC procedure.
ALL_SLICE_FAILED	403 Forbidden	All S-NSSAIs are failed in the NSAC procedure, e.g. due to exceed the configured maximum number of UEs.

6.1.8 Feature negotiation

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

Table 6.1.8-1: Supported Features

Feature number	Feature Name	Description

6.1.9 Security

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

The Nnsacf_NSAC API defines a single scope nnsacf-nsac" for the entire service, and it does not define any additional scopes at resource or operation level.

6.2 Nnsacf_SliceEventExposure Service API

6.2.1 Introduction

The Nnsacf_SliceEventExposure shall use the Nnsacf_SliceEventExposure API.

The API URI of the Nnsacf_SliceEventExposure 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 "nnsacf-slice-ee".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 6.2.3.

6.2.2 Usage of HTTP

6.2.2.1 General

HTTP/2, IETF RFC 7540 [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 Nnsacf_SliceEventExposure API is contained in Annex A.

6.2.2.2 HTTP standard headers

6.2.2.2.1 General

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

6.2.2.2.2 Content type

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

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [13].

6.2.2.3 HTTP custom headers

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

6.2.3 Resources

6.2.3.1 Overview

The figure 6.2.3.1-1 describes the resource URI structure of the Nnsacf_SliceEventExposure API.

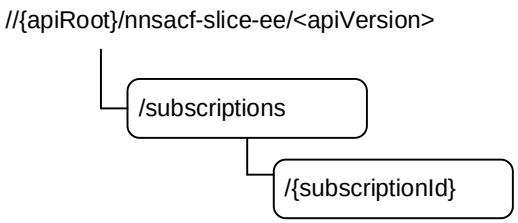

Figure 6.2.3.1-1: Resource URI structure of the Nnsacf_SliceEventExposure API

Table 6.2.3.1-1 provides an overview of the resources and applicable HTTP methods.

Table 6.2.3.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Subscriptions Collection (Collection)	/subscriptions	POST	Mapped to the service operation Subscribe, when to create a subscription
Individual subscription	/subscriptions/{subscriptionId}	PATCH	Mapped to the service operation Subscribe, when to modify the subscription partially
		PUT	Mapped to the service operation Subscribe, when to modify the subscription completely
		DELETE	Mapped to the service operation Unsubscribe

6.2.3.2 Resource: Subscriptions collection

6.2.3.2.1 Description

This resource represents a collection of subscriptions created by NF service consumers of Nnsacf_SliceEventExposure service.

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

6.2.3.2.2 Resource Definition

Resource URI: **{apiRoot}/nnsacf-slice-ee/<apiVersion>/subscriptions**

This resource shall support the resource URI variables defined in table 6.2.3.2.2-1.

Table 6.2.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.2.1
apiVersion	string	See clause 6.2.1.

6.2.3.2.3 Resource Standard Methods

6.2.3.2.3.1 POST

This method shall support the URI query parameters specified in table 6.2.3.2.3.1-1.

Table 6.2.3.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 6.2.3.2.3.1-2 and the response data structures and response codes specified in table 6.2.3.2.3.1-3.

Table 6.2.3.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SACEventSubscription	M	1	Represents the subscription to the events for slice admission control

Table 6.2.3.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
CreatedSACEventSubscription	M	1	201 Created	Represents successful creation of the events subscription for slice admission control
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
ProblemDetails	O	0..1	403 Forbidden	Indicates the creation of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SLICE_NOT_FOUND
NOTE: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.3.2.3.1-4: 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}/nnsacf-slice-ee/<apiVersion>/subscriptions/{subscriptionId}

Table 6.2.3.2.3.1-5: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.2.3.2.3.1-6: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.2.3.2.4 Resource Custom Operations

In this release of this specification, no custom operations associated to this resource is defined.

6.2.3.3 Resource: Individual subscription

6.2.3.3.1 Description

This resource represents an individual of subscription created by NF service consumers of Nnsacf_SliceEventExposure service.

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

6.2.3.3.2 Resource Definition

Resource URI: **{apiRoot}/nnsacf-slice-ee/<apiVersion>/subscriptions/{subscriptionId}**

This resource shall support the resource URI variables defined in table 6.2.3.3.2-1.

Table 6.2.3.3.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 6.2.1
apiVersion	string	See clause 6.2.1.
subscriptionId	string	String identifies an individual subscription to the NSACF event exposure service

6.2.3.3.3 Resource Standard Methods

6.2.3.3.3.1 PATCH

This method shall support the URI query parameters specified in table 6.2.3.3.3.1-1.

Table 6.2.3.3.3.1-1: 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 6.2.3.3.3.1-2 and the response data structures and response codes specified in table 6.2.3.3.3.1-3.

Table 6.2.3.3.3.1-2: 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 [14].

Table 6.2.3.3.3.1-3: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
CreatedSACEventSubscription	M	1	200 OK	Represents successful update of the events subscription for slice admission control
n/a			204 No Content	Represents a successful update of the events subscription for slice admission control, and no information needs to be returned to the NF service consumer.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
ProblemDetails	O	0..1	403 Forbidden	Indicates the modification of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SLICE_NOT_FOUND
ProblemDetails	O	0..1	404 Not Found	Indicates the modification of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SUBSCRIPTION_NOT_FOUND
NOTE: The manadatory HTTP error status code for the PATCH method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.3.3.3.1-4: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.2.3.3.3.1-5: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.2.3.3.3.2 PUT

This method shall support the URI query parameters specified in table 6.2.3.3.3.2-1.

Table 6.2.3.3.3.2-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 6.2.3.3.3.2-2 and the response data structures and response codes specified in table 6.2.3.3.3.2-3.

Table 6.2.3.3.3.2-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
SACEventSubscription	M	1	Represents the events subscription for slice admission control to be completely replaced.

Table 6.2.3.3.3.2-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
CreatedSACEventSubscription	M	1	200 OK	Represents successful update of the events subscription for slice admission control.
n/a			204 No Content	Represents the events subscription modification provided by the NF Service Consumer is accepted entirely.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
ProblemDetails	O	0..1	403 Forbidden	Indicates the creation of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SLICE_NOT_FOUND
ProblemDetails	O	0..1	404 Not Found	Indicates the modification of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SUBSCRIPTION_NOT_FOUND
NOTE: The manadatory HTTP error status code for the PUT method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.3.3.3.2-4: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.2.3.3.3.2-5: 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 NSACF or NSACF (service) set. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.2.3.3.3.3 DELETE

This method shall support the URI query parameters specified in table 6.2.3.3.3.3-1.

Table 6.2.3.3.3.3-1: 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 6.2.3.3.3.3-2 and the response data structures and response codes specified in table 6.2.3.3.3.3-3.

Table 6.2.3.3.3.3-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 6.2.3.3.3.3-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Upon success, an empty response body shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an alternative URI of the resource located on an alternative service instance within the same NSACF or NSACF (service) set.
ProblemDetails	O	0..1	404 Not Found	Indicates the modification of subscription has failed due to application error. The "cause" attribute may be used to indicate one of the following application errors: - SUBSCRIPTION_NOT_FOUND.
NOTE: The manadatory HTTP error status code for the DELETE method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.3.3.3.3-4: 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 another NF service consumer to which the notification should be sent. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.2.3.3.3.3-5: 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 another NF service consumer to which the notification should be sent. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.2.3.3.4 Resource Custom Operations

In this release of this specification, no custom operations associated to this resource is defined.

6.2.4 Custom Operations without associated resources

In this release of this specification, no custom operations without associated resources are defined.

6.2.5 Notifications

6.2.5.1 General

This clause specifies the notifications provided by the Nnsacf_SliceEventExposure service.

Table 6.2.5.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
NSACF Event Notification	{eventNotifyUri}	POST	

6.2.5.2 NSACF Event Notification

If a NF service consumer has subscribed to an event(s) supported by Nnsacf_SliceEventExposure service, when NSACF aware of a state change of the event, NSACF shall create a notification including the event state report, and shall deliver the notification to the call-back URI, following Subscribe/Notify mechanism defined in 3GPP TS 29.501 [5].

6.2.5.2.1 Notification Definition

Call-back URI: **{callbackUri}**

Call-back URI is "eventNotifyUri" provided by NF Service Consumer during creation of the subscription.

6.2.5.2.2 Notification Standard Methods

6.2.5.2.2.1 POST

This method shall support the request data structures specified in table 6.2.5.2.2.1-1 and the response data structures and response codes specified in table 6.2.5.2.2.1-2.

Table 6.2.5.2.2.1-2: Data structures supported by the POST Request Body

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

Table 6.2.5.2.2.1-3: Data structures supported by the POST Response Body

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Upon success, an empty response body shall be returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an URI pointing to the endpoint of another NF service consumer to which the notification should be sent.
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing a different URI, or the same URI if this is a redirection triggered by an SCP to the same target resource via another SCP. In the former case, the URI shall be an URI pointing to the endpoint of another NF service consumer to which the notification should be sent.
NOTE: The manadatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.				

Table 6.2.5.2.2.1-4: 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 another NF service consumer to which the notification should be sent. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

Table 6.2.5.2.2.1-5: 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 another NF service consumer to which the notification should be sent. Or the same URI, if a request is redirected to the same target resource via a different SCP.
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the request is redirected

6.2.6 Data Model

6.2.6.1 General

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

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

Table 6.2.6.1-1: Nnsacf_SliceEventExposure specific Data Types

Data type	Clause defined	Description	Applicability
SACEventSubscription	6.2.6.2.2	Request data to create the event subscription	
CreatedSACEventSubscription	6.2.6.2.3	Response data on created event subscription	
SACEventReport	6.2.6.2.4	Event notification	
SACEvent	6.2.6.2.5	Describes an event to be subscribed	
SACEventReportItem	6.2.6.2.6	Represents a report triggered by a subscribed event type	
SACEventState	6.2.6.2.7	Represents the state of a subscribed event	
SACEventType	6.2.6.3.3	Describes the supported event types	
SACEventTrigger	6.2.6.3.4	Describes how NSACF should generate the report for the event	

Table 6.2.6.1-2 specifies data types re-used by the Nnsacf_SliceEventExposure service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nnsacf_SliceEventExposure service based interface.

Table 6.2.6.1-2: Nnsacf_SliceEventExposure re-used Data Types

Data type	Reference	Comments	Applicability
PatchItem	3GPP TS 29.571 [16]		
Uri	3GPP TS 29.571 [16]	Callback URI	
NfInstanceId	3GPP TS 29.571 [16]	NF Instance Id	
DurationSec	3GPP TS 29.571 [16]	Time value in seconds	
SACInfo	3GPP TS 29.571 [16]	SAC Information	
DateTime	3GPP TS 29.571 [16]	UTC time	
SupportedFeatures	3GPP TS 29.571 [16]	Supported Features	
Snssai	3GPP TS 29.571 [16]	S-NSSAI	
SACEventStatus	3GPP TS 29.571 [16]	SAC Event Status	

6.2.6.2 Structured data types

6.2.6.2.1 Introduction

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

6.2.6.2.2 Type: SACEventSubscription

Table 6.2.6.2.2-1: Definition of type SACEventSubscription

Attribute name	Data type	P	Cardinality	Description	Applicability
event	SACEvent	M	1	Describes the event to be subscribed in subscription request.	
eventNotifyUri	Uri	M	1	Identifies the recipient of notifications sent by NSACF for this subscription.	
nfId	NfInstanceId	M	1	Indicates the instance identity of the network function creating the subscription.	
notifyCorrelationId	string	C	0..1	This IE shall be present if available. If present, this IE identifies the notification correlation ID. The NSACF shall include this ID in the notifications. The value of this IE shall be unique per subscription for a given NF service consumer.	
maxReports	integer	C	0..1	This IE shall be present if available. If present, this IE contains the maximum number of reports that can be generated by each subscribed event in the subscription.	
expiry	DateTime	C	0..1	This IE shall be included in an event subscription response, if, based on operator policy and taking into account the expiry time included in the request, the NSACF needs to include an expiry time. This IE may be included in an event subscription request. When present, this IE shall represent the time after which the subscribed event(s) shall stop generating report and the subscription becomes invalid. This IE shall be absent in the response for one time and immediate reporting (see clause 5.3.2.2.4).	
supportedFeatures	SupportedFeatures	C	0..1	This IE shall be present if at least one optional feature defined in clause 6.3.8 is supported.	

6.2.6.2.3 Type: CreatedSACEventSubscription

Table 6.2.6.2.3-1: Definition of type CreatedSACEventSubscription

Attribute name	Data type	P	Cardinality	Description	Applicability
subscription	SACEventSubscription	M	1	Represents the newly created SAC Event Subscription resource.	
subscriptionId	string	M	1	Represents the subscription Id of the newly created SAC Event Subscription resource.	
report	SACEventReportItem	C	0..1	This IE shall be present if available and if the immediateFlag attribute is set to "true" in subscription request. When present, this IE represents the immediate event report (i.e. the current value of the event subscribed).	
supportedFeatures	SupportedFeatures	C	0..1	This IE shall be present if at least one optional feature defined in clause 6.3.8 is supported.	

6.2.6.2.4 Type: SACEventReport

Table 6.2.6.2.4-1: Definition of type SACEventReport

Attribute name	Data type	P	Cardinality	Description	Applicability
report	SACEventReportItem	M	1	This IE represents the event report to be delivered.	
notifyCorrelationId	string	C	0..1	This IE shall be present if available. If present, this IE 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.	

6.2.6.2.5 Type: SACEvent

Table 6.2.6.2.5-1: Definition of type SACEvent

Attribute name	Data type	P	Cardinality	Description	Applicability
eventType	SACEventType	M	1	Describes the event type to be reported.	
eventTrigger	SACEventTrigger	C	0..1	Describes how the reports are triggered. (See NOTE 1)	
eventFilter	array(Snssai)	M	1..N	This IE shall indicate the S-NSSAI list to be applied.	
notificationPeriod	DurationSec	C	0..1	This IE shall be present if the eventTrigger is set to "PERIODIC". When present, this IE contains the time period for the event reports.	
notifThreshold	SACInfo	C	0..1	This IE shall be present if the eventTrigger is set to "THRESHOLD". When present, this IE Indicates the monitoring threshold value, upon which event notification(s) are triggered.	
immediateFlag	boolean	O	0..1	This attribute shall be set to "true" to indicate an immediate event report in the subscription response is requested. The report contains the current value of the event stored at the time of the subscription in the NSACF. (See NOTE)	
NOTE 1: The eventTrigger shall not be present if the maxReports attribute in the SACEventSubscription is set to 1. Otherwise, the eventTrigger shall be present. NOTE 2: If the immediateFlag flag is absent or set to "false", then the immediate reporting shall not be done.					

6.2.6.2.6 Type: SACEventReportItem

Table 6.2.6.2.6-1: Definition of type SACEventReportItem

Attribute name	Data type	P	Cardinality	Description	Applicability
eventType	SACEventType	M	1	Describes the type of the event which triggers the report	
eventState	SACEventState	M	1	Describes the state of the event which triggered the report.	
timeStamp	DateTime	M	1	This IE shall contain the time at which the event is generated.	
eventFilter	Snssai	M	1	This IE shall indicate the S-NSSAI to be applied.	
sliceStautsInfo	SACEventStatus	C	0..1	If the "eventType" attribute is set to "NUM_OF_REGD_UES" or "NUM_OF_ESTD_PDU_SESSIONS", this parameter shall be included to indicate the current network slice status information for the concerned network slice. (NOTE)	
NOTE: For periodic reporting, both of the values expressed in percentage and in numerical shall be included.					

6.2.6.2.7 Type: SACEventState

Table 6.2.6.2.7-1: Definition of type SACEventState

Attribute name	Data type	P	Cardinality	Description	Applicability
active	boolean	M	1	Represents the active state of the subscribe event. "TRUE" value indicates the event will continue generating reports; "FALSE" value indicates the event will not generate further report.	
remainReports	integer	O	0..1	Represents the number of remain reports to be generated by the subscribed event.	
remainDuration	DurationSec	O	0..1	Represents how long the subscribed event will continue generating reports.	

6.2.6.3 Simple data types and enumerations

6.2.6.3.1 Introduction

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

6.2.6.3.2 Simple data types

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

Table 6.2.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability

6.2.6.3.3 Enumeration: SACEventType

Table 6.2.6.3.3-1: Enumeration SACEventType

Enumeration value	Description	Applicability
"NUM_OF_REGD_UES"	A NF subscribes to this event to receive the current number of registered UEs for a network slice.	
"NUM_OF_ESTD_PDU_SESSIONS"	A NF subscribes to this event to receive the current number of established PDU Sessions for a network slice.	

6.2.6.3.4 Enumeration: SACEventTrigger

Table 6.2.6.3.4-1: Enumeration SACEventTrigger

Enumeration value	Description	Applicability
"THRESHOLD"	Defines that the NSACF should generate reports for the event when the defined threshold value is reached, until the subscription to this event ends: - due to end of report duration or - up to the maximum number of reports or - the event being unsubscribed explicitly.	
"PERIODIC"	Defines that the NSACF should periodically generate reports for the event, until the subscription to this event ends: - due to end of report duration or - up to the maximum number of reports or - the event being unsubscribed explicitly.	

6.2.6.4 Data types describing alternative data types or combinations of data types

In this release, no alternative data types or combinations of data types are defined in this specification.

6.2.6.5 Binary data

In this release, no binary data types are defined in this specification.

6.2.7 Error Handling

6.2.7.1 General

For the Nnsacf_SliceEventExposure 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 Nnsacf_SliceEventExposure API.

6.2.7.2 Protocol Errors

No specific procedures for the Nnsacf_SliceEventExposure service are specified.

6.2.7.3 Application Errors

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

Table 6.2.7.3-1: Application errors

Application Error	HTTP status code	Description
SLICE_NOT_FOUND	403 Forbidden	The given S-NSSAI is not found by the NSACF in the list of S-NSSAIs which are subjected to NSAC procedure.

6.2.8 Feature negotiation

The optional features in table 6.3.8-1 are defined for the Nnsacf_SliceEventExposure API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.2.8-1: Supported Features

Feature number	Feature Name	Description

6.2.9 Security

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

The Nnsacf_SliceEventExposure API defines a single scope "nnsacf-slice-ee" for the entire service, and it does not define any additional scopes at resource or operation level.

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 3GPP TS 29.501 [5] clause 5.3.1 and 3GPP TR 21.900 [7] clause 5B).

A.2 Nnsacf_NSAC API

```
openapi: 3.0.0

info:
  title: Nnsacf_NSAC
  version: 1.0.0
  description: |
    Nnsacf_NSAC Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.536 V17.1.0; 5G System; Network Slice Admission Control Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.536/

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

security:
  - {}
  - oAuth2ClientCredentials:
    - nnsacf-nsac

paths:
  /slices/ues:
    post:
      summary: Network Slice Admission Control on the Number of UEs
      operationId: NumOfUEsUpdate
      tags:
        - slice collection
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/UeACRequestData'
        required: true
      responses:
        '200':
          description: Partial successful ACU operation
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/UeACResponseData'
```

```
        '204':
          description: Successful ACU operation
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          description: Unsucessful ACU operation - Bad Request
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '403':
          description: Unsuccessful ACU operation – Slice Not Subject to NSAC
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '404':
          description: Unsuccessful ACU operation – Slice Not Found
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        '504':
          $ref: 'TS29571_CommonData.yaml#/components/responses/504'
      callbacks:
        eacNotification:
          '{request.body#/eacNotificationUri}':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/EacNotification'
              responses:
                '204':
                  description: slice re-authentication notification response
                '307':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/307'
                '308':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/308'
                '400':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/400'
                '404':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
                '500':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/503'
                default:
                  description: Unexpected error

  /slices/pdus:
    post:
      summary: Network Slice Admission Control on the number of PDU Sessions
      operationId: NumOfPDUsUpdate
      tags:
        - slice collection
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PduACRequestData'
        required: true
      responses:
        '200':
          description: Partial successful ACU operation
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PduACResponseData'
        '204':
```

```
          description: Successful ACU operation
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          description: Unsucessful ACU operation - Bad Request
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '403':
          description: Unsuccessful ACU operation – Slice Not Subject to NSAC
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '404':
          description: Unsuccessful ACU operation – Slice Not Found
          content:
            application/problem+json:
              schema:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        '504':
          $ref: 'TS29571_CommonData.yaml#/components/responses/504'

components:

  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nnsacf-nsac: Access to the Nnsacf_NSAC API

  schemas:

    #
    # STRUCTURED DATA TYPES:
    #

    UeACRequestData:
      type: object
      properties:
        ueACRequestInfo:
          type: array
          items:
            $ref: '#/components/schemas/UeACRequestInfo'
          minItems: 1
        nfId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
        nfType:
          $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/NFType'
        eacNotificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
      required:
        - ueACRequestInfo
        - nfId

    UeACRequestInfo:
      type: object
      properties:
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        anType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        acuOperationList:
          type: array
          items:
            $ref: '#/components/schemas/AcuOperationItem'
          minItems: 1
        additionalAnType:
```

```
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
    required:
      - supi
      - anType
      - acuOperationList

  UeACResponseData:
    type: object
    properties:
      acuFailureList:
        description: A map (list of key-value pairs) where the key of the map shall be UE's supi
        type: object
        additionalProperties:
          type: array
          items:
            $ref: '#/components/schemas/AcuFailureItem'
          minItems: 1
        minProperties: 1

  AcuOperationItem:
    type: object
    properties:
      updateFlag:
        $ref: '#/components/schemas/AcuFlag'
      snssai:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
      plmnId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnId'
    required:
      - updateFlag
      - snssai

  AcuFailureItem:
    type: object
    properties:
      snssai:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
      reason:
        $ref: '#/components/schemas/AcuFailureReason'
      plmnId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnId'
      pduSessionId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
    required:
      - snssai

  EacNotification:
    description: A map (list of key-value pairs) where Snssai converted to a string serves as key
    type: object
    additionalProperties:
      $ref: '#/components/schemas/EACMode'
    minProperties: 1

  PduACRequestData:
    type: object
    properties:
      pduACRequestInfo:
        type: array
        items:
          $ref: '#/components/schemas/PduACRequestInfo'
        minItems: 1
      nfId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
      pgwFqdn:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Fqdn'
    required:
      - pduACRequestInfo

  PduACRequestInfo:
    type: object
    properties:
      supi:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
      anType:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
      pduSessionId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
      acuOperationList:
```

```
        type: array
        items:
          $ref: '#/components/schemas/AcuOperationItem'
        minItems: 1
        maxItems: 2
      additionalAnType:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
    required:
      - supi
      - anType
      - pduSessionId
      - acuOperationList

  PduACResponseData:
    type: object
    properties:
      acuFailureList:
        description: A map (list of key-value pairs) where the key of the map shall be UE's supi
        type: object
        additionalProperties:
          type: array
          items:
            $ref: '#/components/schemas/AcuFailureItem'
          minItems: 1
          maxItems: 2
        minProperties: 1

  #
  # SIMPLE DATA TYPES
  #


  #
  # ENUMERATIONS
  #

  EACMode:
    anyOf:
    - type: string
      enum:
        - ACTIVE
        - DEACTIVE
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.
    description: >
      EAC mode. Possible values are
      - ACTIVE
      - DEACTIVE

  AcuFlag:
    anyOf:
    - type: string
      enum:
        - INCREASE
        - DECREASE
        - UPDATE
    - type: string
      description: >
        This string provides forward-compatibility with future
        extensions to the enumeration but is not used to encode
        content defined in the present version of this API.
    description: >
      Update Flag of ACU operation. Possible values are
      - INCREASE
      - DECREASE
      - UPDATE

  AcuFailureReason:
    anyOf:
    - type: string
      enum:
        - SLICE_NOT_FOUND
        - EXCEED_MAX_UE_NUM
        - EXCEED_MAX_UE_NUM_3GPP
        - EXCEED_MAX_UE_NUM_N3GPP
```

```
          - EXCEED_MAX_PDU_NUM
          - EXCEED_MAX_PDU_NUM_3GPP
          - EXCEED_MAX_PDU_NUM_N3GPP
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Failure Reason of ACU operation to an S-NSSAI. Possible values are
        - SLICE_NOT_FOUND
        - EXCEED_MAX_UE_NUM
        - EXCEED_MAX_UE_NUM_3GPP
        - EXCEED_MAX_UE_NUM_N3GPP
        - EXCEED_MAX_PDU_NUM
        - EXCEED_MAX_PDU_NUM_3GPP
        - EXCEED_MAX_PDU_NUM_N3GPP
```

A.3 Nnsacf_SliceEventExposure API

```
openapi: 3.0.0

info:
  title: Nnsacf_SliceEventExposure
  version: 1.0.0
  description: |
    Nnsacf_SliceEventExposure Service.
    © 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.536 V17.1.0; 5G System; Network Slice Admission Control Services; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.536/

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

security:
  - {}
  - oAuth2ClientCredentials:
    - nnsacf-slice-ee

paths:
  /subscriptions:
    post:
      summary: Nnsacf_SliceEventExposure Subscribe service Operation
      tags:
        - Subscriptions collection (Collection)
      operationId: CreateSubscription
      requestBody:
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SACEventSubscription'
        required: true
      responses:
        '201':
          description: Subsription Created
          headers:
            Location:
              description: 'Contains the URI of the newly created resource, according to the
structure: {apiRoot}/nnsacf-slice-ee/<apiVersion>/subscriptions/{subscriptionId}'
              required: true
              schema:
                type: string
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/CreatedSACEventSubscription'
        '307':
```

```
        $ref: 'TS29571_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29571_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '403':
        $ref: 'TS29571_CommonData.yaml#/components/responses/403'
      '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'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        description: Unexpected error
    callbacks:
      eventReport:
        '{$request.body#/subscription/eventNotifyUri}':
          post:
            summary: Event Notificaiton Delivery
            requestBody:
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/SACEventReport'
              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'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                description: Unexpected error

  /subscriptions/{subscriptionId}:
    patch:
      summary: Nnsacf_SliceEventExposure Subscribe partial modify service Operation
      tags:
        - Individual subscription (Document)
      operationId: PartialModifySubscription
      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: Subsription modified successfully
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/CreatedSACEventSubscription'
      '307':
        $ref: 'TS29571_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29571_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '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'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        description: Unexpected error
  put:
    summary: Nnsacf_SliceEventExposure Subscribe complete modify service Operation
    tags:
      - Individual subscription (Document)
    operationId: CompleteModifySubscription
    parameters:
      - name: subscriptionId
        in: path
        required: true
        description: Unique ID of the subscription to be modified
        schema:
          type: string
    requestBody:
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/SACEventSubscription'
      required: true
    responses:
      '200':
        description: Subsription modified successfully
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/CreatedSACEventSubscription'
      '204':
        description: Events subscription modification is accepted entirely
      '307':
        $ref: 'TS29571_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29571_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29571_CommonData.yaml#/components/responses/400'
      '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'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          description: Unexpected error
    delete:
      summary: Nnsacf_SliceEventExposure Unsubscribe service Operation
      tags:
        - Individual subscription (Document)
      operationId: DeleteSubscription
      parameters:
        - name: subscriptionId
          in: path
          required: true
          description: Unique ID of the subscription to be deleted
          schema:
            type: string
      responses:
        '204':
          description: Subsription 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'
        '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'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          description: Unexpected error

components:

  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            nnsacf-slice-ee: Access to the Nnsacf_SliceEventExposure API

  schemas:

    #
    # STRUCTURED DATA TYPES
    #

    SACEventSubscription:
      description: Request data to create the event subscription
      type: object
      required:
        - event
        - eventNotifyUri
        - nfId
      properties:
        event:
          $ref: '#/components/schemas/SACEvent'
        eventNotifyUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        nfId:
```

```
        $ref: 'TS29571_CommonData.yaml#/components/schemas/NfInstanceId'
      notifyCorrelationId:
        type: string
      maxReports:
        type: integer
      expiry:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
      supportedFeatures:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'

  CreatedSACEventSubscription:
    description: Response data on created event subscription
    type: object
    required:
      - subscription
      - subscriptionId
    properties:
      subscription:
        $ref: '#/components/schemas/SACEventSubscription'
      subscriptionId:
        type: string
      report:
        $ref: '#/components/schemas/SACEventReportItem'
      supportedFeatures:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'

  SACEventReport:
    description: Event notification
    type: object
    required:
      - report
    properties:
      report:
        $ref: '#/components/schemas/SACEventReportItem'
      notifyCorrelationId:
        type: string

  SACEvent:
    description: Describes an event to be subscribed
    type: object
    required:
      - eventType
      - eventFilter
    properties:
      eventType:
        $ref: '#/components/schemas/SACEventType'
      eventTrigger:
        $ref: '#/components/schemas/SACEventTrigger'
      eventFilter:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        minItems: 1
      notificationPeriod:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
      notifThreshold:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SACInfo'
      immediateFlag:
        type: boolean
        default: false

  SACEventReportItem:
    description: Represents a report triggered by a subscribed event type
    type: object
    required:
      - eventType
      - eventState
      - timeStamp
      - eventFilter
    properties:
      eventType:
        $ref: '#/components/schemas/SACEventType'
      eventState:
        $ref: '#/components/schemas/SACEventState'
      timeStamp:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
      eventFilter:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
```

```
      sliceStautsInfo:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SACEventStatus'

  SACEventState:
    description: Represents the state of a subscribed event
    type: object
    required:
      - active
    properties:
      active:
        type: boolean
      remainReports:
        type: integer
      remainDuration:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'

  #
  # SIMPLE DATA TYPES
  #


  #
  # ENUMERATIONS
  #

  SACEventType:
    description: Describes the supported event types
    anyOf:
    - type: string
      enum:
        - NUM_OF_REGD_UES
        - NUM_OF_ESTD_PDU_SESSIONS
    - type: string

  SACEventTrigger:
    description: Describes how NSACF should generate the report for the event
    anyOf:
    - type: string
      enum:
        - THRESHOLD
        - PERIODIC
    - type: string
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-04	CT4#103E	C4-212108				TS skeleton	0.0.1
2021-04	CT4#103E	C4-212430, etc.				Implementation of pCRs agreed in CT4#103E (C4-212430, C4-212610, C4-212432, C4-212112)	0.1.0
2021-06	CT4#104E	C4-213440, etc.				Implementation of pCRs agreed in CT4#104E (C4-213440, C4-213441, C4-213442, C4-213443, C4-213444, C4-213445, C4-213446, C4-213435, C4-213436, C4-213437, C4-213438)	0.2.0
2021-09	CT4#105E	C4-214694, etc.				Implementation of pCRs agreed in CT4#105E (C4-214694, C4-214695, C4-214645, C4-214646, C4-214647, C4-214098, C4-214610, C4-214611, C4-214107, C4-214292, C4-214593, C4-214594, C4-214595, C4-214317, C4-214318, C4-214729, C4-214730, C4-214337)	0.3.0
2021-10	CT4#106E	C4-215382, etc.				Implementation of pCRs agreed in CT4#106E (C4-215382, C4-215116, C4-215470, C4-215383, C4-215385, C4-215386, C4-215388, C4-215389, C4-215390, C4-215391, C4-215392, C4-215393, C4-215394, C4-215395, C4-215525, C4-215415, C4-215416, C4-215264)	0.4.0
2021-11	CT4#107E	C4-216052, etc.				Implementation of pCRs agreed in CT4#107E (C4-216052, C4-216240, C4-216241, C4-216414, C4-216415, C4-216416, C4-216429, C4-216446, C4-216516)	0.5.0
2021-12	CT#94e	CP-213155				V1.0.0 presented for information	1.0.0
2022-01	CT4#107bis-E	C4-220378, etc.				Implementation of pCRs agreed in CT4#107bis-E (C4-220379, C4-220357, C4-220459, C4-220070, C4-220389, C4-220345, C4-220346, C4-220348, C4-220372, C4-220411, C4-220413, C4-220284)	1.1.0
2022-03	CT4#108-E	C4-221040, etc.				Implementation of pCRs agreed in CT4#108-E (C4-221040, C4-221046, C4-221450, C4-221505, C4-221302)	1.2.0
2022-03	CT#95e	CP-220104				TS presented for approval	2.0.0
2022-03	CT#95e					TS approved	17.0.0
2022-06	CT#96	CP-221033	0003	1	F	NSAC for emergency and priority sessions alignment	17.1.0
2022-06	CT#96	CP-221033	0005	1	F	Session continuity guarantee with multiple NSACFs deployment	17.1.0
2022-06	CT#96	CP-221038	0008	-	F	Consumers of NSACF event exposure service	17.1.0
2022-06	CT#96	CP-221028	0010	1	F	Reuse of type Fqdn from 29.571	17.1.0
2022-06	CT#96	CP-221033	0011	1	F	Clarification on Per Access NSAC	17.1.0
2022-06	CT#96	CP-221033	0012	1	F	Removal of NSACF from HPLMN in LBO Model	17.1.0
2022-06	CT#96	CP-221051	0013	-	F	API version and External doc update	17.1.0
2022-09	CT#97	CP-222028	0014	1	F	Clarification on per access failure reason	17.2.0
2023-06	CT#100	CP-231070	0048	-	F	Correction on the cardinality of acuFailureList	17.3.0
2023-12	CT#102	CP-233064	0090	1	F	Essential Correction on PDU Session ID in NumOfPDUsUpdate	17.4.0

History

Document history		
V17.0.0	May 2022	Publication
V17.1.0	July 2022	Publication
V17.2.0	October 2022	Publication
V17.3.0	July 2023	Publication
V17.4.0	January 2024	Publication