ETSI TS 124 549 V18.1.0 (2024-05)

5G;
Network slice capability enablement- Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification;
Stage 3
(3GPP TS 24.549 version 18.1.0 Release 18)

Reference
RTS/TSGC-0124549vi10

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 the 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 protocol aspects of the SEAL service for the network slice capability enablement to support re-mapping of a vertical application to different slices over the 3GPP system and slice capabilities based on 5GS management system services and 5GS network services. The protocol aspects specify the User Equipment (UE) supporting the client functionality of this SEAL service and the network supporting the server functionality of this SEAL service, where the client functionality and server functionality are specified in 3GPP TS 23.434 [2] and 3GPP TS 23.435 [13].

The present document is also applicable to the application server supporting the Vertical Application Layer server (VAL server) functionality for a specific Vertical Application Layer service (VAL service). The specification for the VAL server for a specific VAL service is out of scope of the present document.

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 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[2A] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[3] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[3A] 3GPP TS 24.546: "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[4] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[5] Void.

[6] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[7] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[8] IETF RFC 9110:"HTTP Semantics".

[9] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

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

[11] IETF RFC 8323: "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets".

[12] OMA OMA-TS-XDM_Core-V2_1-20120403-A: "XML Document Management (XDM) Specification".

[13] 3GPP TS 23.435: "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service".

[14] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[15] 3GPP TS 26.531: "Data Collection and Reporting; General Description and Architecture".

[16] 3GPP TS 26.532: "Data Collection and Reporting; Protocols and Formats".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

SEAL network slice capability enablement client: An entity that provides the client side functionalities corresponding to the SEAL network slice capability enablement service.

SEAL network slice capability enablement server: An entity that provides the server side functionalities corresponding to the SEAL network slice capability enablement service.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.434 [2] apply:

SEAL client
SEAL server
SEAL service
VAL server
VAL service
VAL user
Vertical
Vertical application

For the purposes of the present document, the following terms and definitions given in 3GPP TS 26.532 [16] apply:

Data Collection Client
Data Collection AF

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].

5GCN	5G Core Network
AF	Application Function
DNN	Data Network Name
HTTP	Hypertext Transfer Protocol
KQI	Key Quality Indicator
NSCE	Network Slice Capability Enablement
PCF	Policy Control Function
QoE	Quality of Experience
SEAL	Service Enabler Architecture Layer
SNSCE-C	SEAL Network Slice Capability Enablement Client
SNSCE-S	SEAL Network Slice Capability Enablement Server
S-NSSAI	Single Network Slice Selection Assistance Information
UE	User Equipment
URSP	UE Route Selection Policy
VAL	Vertical Application Layer
XCAP	XML Configuration Access Protocol
XDMC	XML Document Management Client
XDMC	XML Document Management Server
XML	Extensible Markup Language

4 General description

The present document enables a SEAL Network Slice Capability Enablement Client (SNSCE-C) and a Vertical Application Layer server (VAL server) that communicate with a SEAL Network Slice Capability Enablement Server (SNSCE-S). The network slice capability enablement is a SEAL service that provides the network slice capability enablement related capabilities to one or more vertical applications.

In a trusted network, the network slice capability enablement can be used to re-map a vertical application to different slices based on the configuration of the SNSCE-S for updating the application traffic. Therefore, the SNSCE-S acts as an Application Function (AF) and influences the UE's URSP rules for the application traffic by providing guidance on the route selection descriptors S-NSSAI and DNN.

NOTE: In this release, S-NSSAI and DNN are only used as the route selection descriptor.

5 Functional entities

5.1 SEAL network slice capability enablement client (SNSCE-C)

The SNSCE-C functional entity acts as the application client for managing network slice capabilities.

To be compliant with the HTTP procedures in the present document the SNSCE-C:

a) shall support the role of XCAP client as specified in IETF RFC 4825 [6];

b) shall support the role of XDMC as specified in OMAOMA-TS-XDM_Core-V2_1 [12];

c) shall support route selection descriptors configuration e.g. S-NSSAI and DNN adaptation due to new requirements or change of requirements for one or more application; and

d) shall support procedure in clause 6.2.2.2.

To be compliant with the CoAP procedures in the present document the SNSCE-C:

a) shall support the role of CoAP client as specified in IETF RFC 7252 [9];

b) should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [11];

c) shall support route selection descriptors configuration e.g. S-NSSAI and DNN adaptation due to new requirements or change of requirements for one or more application; and

d) shall support procedure in clause 6.2.2.4.

NOTE 1: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [4].

NOTE 2: Support for TCP for the CoAP procedures is required if the client connects over the network which blocks or impedes the use of UDP, e.g. when NATs are present in the communication path.

5.2 SEAL network slice capability enablement server (SNSCE-S)

The SNSCE-S is a functional entity which provides slice capability enablement to administer the network slice for one or more vertical applications.

To be compliant with the HTTP procedures in the present document the SNSCE-S shall:

a) shall support the role of XCAP server as specified in IETF RFC 4825 [6];

b) shall support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [12];

c) shall provide the 5GC network a guidance for route selection descriptors to assign new S-NSSAI and DNN;

d) shall support procedure in clause 6.2.1.1; and

e) shall support procedure in clause 6.2.2.3.

To be compliant with the CoAP procedures in the present document the SNSCE-S shall:

a) shall support the role of CoAP client as specified in IETF RFC 7252 [9];

b) shall support CoAP over TCP and Websocket as specified in IETF RFC 8323 [11];

c) shall provide the 5GC network a guidance for route selection descriptors to assign new S-NSSAI and DNN;

d) shall support procedure in clause 6.2.1.2; and

e) shall support procedure in clause 6.2.2.5.

NOTE: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [4].

6 Network slice capability enablement procedures

6.1 General

The network slice capability enablement procedures is a SEAL service of:

a providing network slice capability enablement capabilities for network slice re-mapping from one VAL service to one or more other VAL services, according to 3GPP TS 23.434 [2] and 3GPP TS 23.435 [13]. The network server entity, providing the functionality for the network slice re-mapping, acts as an AF communicating with 5GCN to provide guidance to update and modify the S-NSSAIs and the DNNs of the route selection descriptors of the URSP rules, 3GPP TS 24.526 [3], for one or more application traffics per UE; and

NOTE: In this release, S-NSSAI and DNN are only used as the route selection descriptor.

b providing slice capabilities based on 5GS management system services and 5GS network services, according to 3GPP TS 23.435 [13] e.g., retrieving the KQI data of services, the QoE data, the end user information and fault reports from NSCE client, notifying the slice modification and delivering slice information to NSCE client.

6.2 On-network procedures

6.2.1 General

6.2.1.1 Authenticated identity in HTTP request

Upon receiving an HTTP request from SNSCE-C, the SNSCE-S shall authenticate the identity of the sender of the HTTP request is authorized as specified in 3GPP TS 24.547 [4], and if authentication is successful, the SNSCE-S shall use the identity of the sender of the HTTP request as an authenticated identity.

6.2.1.2 Authenticated identity in CoAP request

Upon receiving a CoAP request from SNSCE-C, the SNSCE-S shall authenticate the identity of the sender of the CoAP request is authorized as specified in 3GPP TS 24.547 [4], and if authentication is successful, the SNSCE-S shall use the identity of the sender of the CoAP request as an authenticated identity.

6.2.2 Event triggered network slice adaptation

6.2.2.1 General

These clauses describes the procedures on the client and server side when a request for network slice configuration is sent by the client to the server. The network slice configuration request may cause a network slice adaptation and sent by the SNSCE-C acting as application client requesting a new or a change in network slice configuration.

6.2.2.2 SNSCE client HTTP procedure

In order to request for the network slice adaptation, the SNSCE-C shall send an HTTP PUT request message according to procedures specified in IETF RFC 9110 [8]. In the HTTP PUT request message, the SNSCE-C:

NOTE: How the requested network slice is known by the SNSCE-C is out of scope of this release.

a) shall set the Request-URI to the URI identifying the SNSCE-S according to the pattern"{apiRoot}/su_nsc/val-services/{valServiceId}/configurations/{configurationId}", where:

   1) {valServiceId} set to the identity of "VAL service ID" of the VAL application; and

   2) {configurationId}set to the identity of "slice adaptation" configuration,

b) shall set the "Host" header field to the URI identifying of SNSCE-S and the port information;

c) shall include an Authorization header field with the "Bearer" authentication scheme set to an access token of the "bearer" token type as specified in IETF RFC 6750 [7];

d) shall include the parameters for:

   1) VAL UEs of the VAL UE List; and

   2) requested S-NSSAI,

   as specified in table A.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [10]; and

e) may include the parameters for:

   1) requested DNN;

   2) requested application requirements containing:

      - time window;

      - location criteria;

      - access type preference;

   - UE IP address preservation indicator; and

   3) configuration cause,

   as specified in table A.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [10].

Editor's note [CR#0017, WID: NSCALE]: Whether to contain the UE IP address preservation indicator depends on the clarification from SA6.

6.2.2.3 SNSCE server HTTP procedure

Upon receipt an HTTP PUT request:

a) with a Request-URI according to "{apiRoot}/su_nsc/val-services/{valServiceId}/configurations/{configurationId} identifying:

1) "valServiceId" identifying the VAL application; and

2) "configurationId" identifying the slice adaptation configuration; and

b) with a body containing:

1) VAL UE list with one or more VAL UEs;

2) requested S-NSSAI;

3) optionally requested DNN;

4) optionally requested application requirements containing:

- time window;

- location criteria;

- access type preference;

- UE IP address preservation indicator; and

5) optionally configuration cause,

the SNSCE-S shall determine the sender identity as specified in clause 6.2.1.1 to confirm whether the sender is authorized or not. If:

a) the sender is not an authorized user, the SNSCE-S shall respond with an HTTP 403 (Forbidden) response message and avoid the rest of steps; or

b) the sender is an authorized user, the SNSCE-S:

1) shall attempt to update the network S-NSSAI for one or more VAL UEs with the identities listed in the VAL UE list for the VAL service, identified by VAL service ID by using the parameters for requested S-NSSAI, requested DNN, requested application requirements and configuration cause from the HTTP PUT request message;

NOTE 1: To update the application traffic, the SNSCE-S can act as an AF and use the reference point N33 as shown in 3GPP TS 23.434 [2] to influence a VAL UE's URSP rules for the application traffic by providing a guidance on the route selection parameters S-NSSAI and DNN as described in clause 4.15.6.10 of 3GPP TS 23.502 [2A].

NOTE 2: Whether and how the SNSCE-S can update the network S-NSSAI for all VAL UEs for the VAL service, is out of the scope of this release.

2) shall send the updated network S-NSSAI and any DNN to the PCF, if the update is successful, 3GPP TS 23.434 [2]; and

3) shall send an HTTP 200 response message containing the successful status or an error response for the failure status of the requested network slice adaptation to the SNSCE-C.

6.2.2.4 SNSCE client CoAP procedure

In order to request for the network slice adaptation, the SNSCE-C shall send a CoAP POST request message. In the CoAP PUT request message, the SNSCE-C:

NOTE: How the requested network slice is known by the SNSCE-C is out of scope of this release.

a) shall set the CoAP URI identifying a network configuration e.g. the network slice adaptation for a given VAL group containing one or more VAL UEs for a given VAL service according to the API URI definition in clause B.2, by setting:

1) the "apiRoot" to the SNSCE-S URI;

2) the "valServiceId" to the value identifying the given VAL service;

3) the "configurationId" to the value identifying the network slice adaptation;

b) shall include:

1) the VAL group ID of the VAL group containing one or more VAL UEs; and

2) the requested S-NSSAI;

c) may include:

1) the requested DNN;

2) requested application requirements containing:

- time window;
- location criteria;
- access type preference;
- UE IP address preservation indicator; and

3) the requested configuration cause;

d) shall set the "Uri-Host" and "Uri-Port" Options to the URI identifying of SNSCE-S and the port information; and

e) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [4].

6.2.2.5 SNSCE server CoAP procedure

Upon receiving a CoAP PUT request, where the CoAP URI of the request identifies a network slice configuration as the network slice adaptation of one or more VAL UEs for a given VAL service as described in Annex B.2, the SNSCE-S shall determine the identity of the sender as specified in clause 6.2.1.2 to confirm whether the sender is authorized or not. If:

a) the sender is not an authorized user, the SNSCE-S shall respond with a CoAP 4.03 (Forbidden) response message and avoid the rest of steps; or

b) the sender is an authorized user, the SNSCE-S:

1) shall attempt to update the network S-NSSAI for one or more VAL UEs with the identities listed in the VAL UE list for the VAL service, identified by VAL service ID by using the parameters for requested S-NSSAI, requested DNN, requested application requirements and configuration cause from the CoAP PUT request message;

NOTE 1: To update the application traffic, the SNSCE-S can act as an AF and use the reference point N33 as shown in 3GPP TS 23.434 [2] to influence a VAL UE's URSP rules for the application traffic by providing a guidance on the route selection descriptors S-NSSAI and DNN as described in clause 4.15.6.10 of 3GPP TS 23.502 [2A].

NOTE 2: Whether and how the SNSCE-S can update the network S-NSSAI for all VAL UEs for the VAL service, is out of the scope of this release.

2) shall send the updated network S-NSSAI and any DNN to the PCF, if the update is successful, 3GPP TS 23.434 [2]; and

3) shall send a CoAP 2.04 (Changed) response message indicating the successful status or an error response for the failure status of the requested network slice adaptation to the SNSCE-C.

6.2.3 Retrieval of data and information

6.2.3.1 General

The procedures on how the NSCE server retrieves network and service related KQI or performance data, QoE data, and fault information from the NSCE client apply for the following NSCE procedures:

a) network slice related performance and analytics monitoring job creation request procedure specified in 3GPP TS 23.435 [13] clause 9.7.2.1;

b) information collection from NSCE server(s) subscribe request and response procedure specified in 3GPP TS 23.435 [13] clause 9.8.2.1;

c) network slice fault management capability exposure procedure specified in 3GPP TS 23.435 [13] clause 9.15.2.1; and

d) slice requirements verification and alignment capability exposure procedure specified in 3GPP TS 23.435 [13] clause 9.16.2.1.

The procedures at the client and server side follow the mechanism specified in clause 5.5 of 3GPP TS 26.531 [15] and HTTP procedures specified in clause 4.3 and clause 7 of 3GPP TS 26.532 [16]. In the procedures, the SNSCE-C acts as the data collection client, and the SNSCE-S acts as data collection AF.

6.2.3.2 SNSCE client HTTP procedure

In order to obtain the configuration of requested data and information for retrieval, the SNSCE-C shall send an HTTP POST request message to invoke Ndcaf_DataReporting_CreateSession service operation as described in 3GPP TS 26.532 [16] clause 4.3.2.2 and 7.2.2.3.1.

In order to update the configuration of requested data and information for retrieval, the SNSCE-C may send an HTTP GET request message to invoke Ndcaf_DataReporting_RetrieveSession service operation as described in 3GPP TS 26.532 [16] clause 4.3.2.3 and 7.2.3.3.1.

After the configuration, the SNSCE-C shall send an HTTP POST request message in accordance with this configuration to invoke Ndcaf_DataReporting_Report service operation as described in 3GPP TS 26.532 [16] clause 4.3.3 and 7.2.3.4.1.

6.2.3.3 SNSCE server HTTP procedure

Upon receipt an HTTP POST request message on Ndcaf_DataReporting_CreateSession service operation, the SNSCE-S shall send HTTP response and provide the configuration of requested data and information for retrieval as described in clause 4.3.2.2 and clause 7.2.2.3.1 of 3GPP TS 26.532 [16].

Upon receipt an HTTP GET request message on Ndcaf_DataReporting_RetrieveSession service operation, the SNSCE-S shall send HTTP response and provide the updated configuration, if available, as described in clause 4.3.2.3 and clause 7.2.3.3.1 of 3GPP TS 26.532 [16].

Upon receipt an HTTP POST request message on Ndcaf_DataReporting_Report service operation, the SNSCE-S shall send HTTP response and may provide the updated configuration as described in clause 4.3.3 and clause 7.2.3.4.1 of 3GPP TS 26.532 [16].

6.2.4 Notify slice modification in Inter-PLMN based slice service continuity

6.2.4.1 General

This clause describes the procedures on the client and server side when a notification of slice modification in inter-PLMN based slice service continuity is sent by the server to the client. The notification helps the VAL UE identify an slice modification related to a VAL application when moving into target service area of target PLMN.

Editor's note [CR#0020, WID: NSCALE]: The API for this procedure needs to be specified.

6.2.4.2 SNSCE server HTTP procedure

In order to notify an slice modification in Inter-PLMN based slice service continuity, the SNSCE-S shall send an HTTP POST request message according to procedures specified in IETF RFC 9110 [8]. In the HTTP POST request message, the SNSCE-S:

a) shall set the Callback-URI to the URI which was given by SNSCE-C in the configuration update event subscription message specified in 3GPP TS 24.546 [3A] clause 6.2.2.1.2 and A.1.2;

b) shall include the parameters for:

   1) VAL service ID;

   2) slice identifier;

   3) PLMN ID; and

   4) target service area

   as specified in table A.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [10]; and

c) may include the parameter for VAL UE ID list as specified in table A.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [10].

6.2.4.3 SNSCE client HTTP procedure

Upon receiving an HTTP POST request over a callback-URI which was given to SNSCE-S, the SNSCE-C:

a) shall send an HTTP 200 (OK) message; and

b) shall notify the VAL client about slice modification in inter-PLMN based slice service continuity for the VAL application identified by VAL service ID.

6.3 Off-network procedures

The off-network procedures are out of scope of the present document in this release of the specification.

Annex A (normative): HTTP resource representation and encoding

A.1 General

The information in this annex provides a description for the HTTP parameters transmitted by the SNSCE-C to the SNSCE-S to trigger a network slice configuration such as the network slice adaptation for one or more VAL UEs within a VAL service.

A.2 Resource representation and APIs for event triggered network slice configuration

A.2.1 ETN_Configuration API

A.2.1.1 API URI

The HTTP URIs used in HTTP requests from SNSCE-C towards the SNSCE-S shall have the Resource URI structure as defined in clause A.2.1.2.1 which is {apiRoot}/su_nsc/<apiVersion>/val-services/{valServiceId}/configurations/{configurationId}, where

a) {valServiceId} is set to the value of the "VAL Service ID" of the VAL application; and

b) {configurationId} is set to the identity of the configuration.

A.2.1.2 Resources

A.2.1.2.1 Overview

The Resource URI structure of the ETN_Configuration API is as shown in Figure A.2.1.2.1-1:

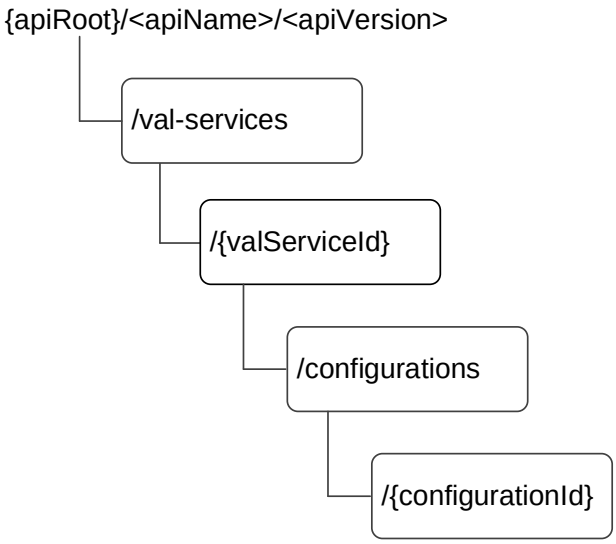

Figure A.2.1.2.1-1: Resource URI structure of the ETN_Configuration API

Table A.2.1.2.1-1 provides an overview of the resources and applicable HTTP method.

Table A.2.1.2.1-1: Resources and method overview

Resource name	Resource URI	HTTP method	Description
Configuration	/val-services/{valServiceId}/configurations/{configurationId}	PUT (NOTE)	Performs configuration.
NOTE: In this release, the only configuration is the slice adaptation as described in 3GPP TS 23.434 [2].			

A.2.1.2.2 Resource: Configuration

A.2.1.2.2.1 Description

The Configuration resource allows an SNSCE-C a specific configuration identified by a configuration ID, to send an HTTP request containing:

a) a list of one or more VAL UEs;

b) a requested S-NSSAI;

c) optionally a requested DNN;

d) optionally the requested application requirements containing:

1) time window;

2) location criteria;

3) access type preference; and

4) UE IP address preservation indicator; and

e) optionally a requested configuration cause,

for a specific VAL service identified by a VAL service ID, toward a SNSCE-S to perform a network triggered slice configuration for the list of one or more VAL UEs for that specific VAL service.

NOTE: In this release, S-NSSAI and DNN are the only used route selection descriptors of the URSP rules described in 3GPP TS 24.526 [3].

A.2.1.2.2.2 Resource Definition

The SNSCE-C uses the parameters shown in table A.2.1.2.2.2-1 to communicate with the SNSCE-S in order to trigger a network slice configuration for one or more VAL UEs within a VAL service.

Table A.2.1.2.2.2-1: Client side parameters for network slice configuration trigger

Parameter	Description
VAL UE List	REQUIRED. Represents a space-separated list of VAL UE Ids within a given VAL service, for which a given network slice configuration trigger applies.
Requested S-NSSAI	REQUIRED. The new S-NSSAI which is requested.
Requested DNN	OPTIONAL. The new DNN which is requested.
Requested application requirements	OPTIONAL. The application-related request parameters.
>Time window	OPTIONAL. Indication of the new scheduled time window that is requested.
>Location criteria	OPTIONAL. Indication of the new location criteria that is requested.
>Access type preference	OPTIONAL. Indication of the new access type (3GPP, non-3GPP or multi-access) preference that is requested.
>UE IP address preservation indicator	OPTIONAL. Indication that UE IP address preservation is requested.
Configuration cause	OPTIONAL. Indicates the cause for the configuration.

Annex B (normative): CoAP resource representation and encoding

B.1 General

The information in this annex provides a description of CoAP resource representation and encoding transmitted by the SNSCE-C to the SNSCE-S to trigger a network configuration i.e. the network slice configuration in this case for one or more VAL UEs within a VAL service.The general rules for resource URI structure, cache usage, error handling and common data types are described in Annex C.1 of 3GPP TS 24.546 [3A].

B.2 Resource representation and APIs for event triggered network slice configuration

B.2.1 ETN_Configuration API

B.2.1.1 API URI

The CoAP URIs used in CoAP requests from SNSCE-C towards the SNSCE-S shall have the Resource URI structure as defined in clause C.1.1 of 3GPP TS 24.546 [3A] with the following clarifications:

- the <apiName> shall be "su_nsc";
- the <apiVersion> shall be "v1"; and
- the <apiSpecificSuffixes> shall be set as described in clause B.2.1.2.

B.2.1.2 Resources

B.2.1.2.1 Overview

The Resource URI structure of the ETN_Configuration API is as shown in Figure B.2.1.2.1-1:

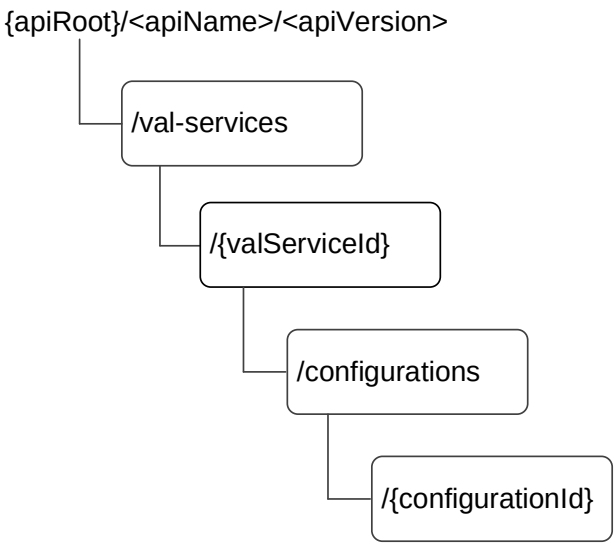

Figure B.2.1.2.1-1: Resource URI structure of the ETN_Configuration API

Table B.2.1.2.1-1 provides an overview of the resources and applicable CoAP method.

Table B.2.1.2.1-1: Resources and method overview

Resource name	Resource URI	CoAP method	Description
Configuration	/val-services/{valServiceId}/configurations/{configurationId}	PUT (NOTE)	Performs configuration.
NOTE: In this release, the only configuration is the slice adaptation as described in 3GPP TS 23.434 [2].			

B.2.1.2.2 Resource: Configuration

B.2.1.2.2.1 Description

The Configuration resource allows an SNSCE-C a specific configuration identified by a configuration ID, to send a CoAP request containing:

a) a list of one or more VAL UEs;

b) a requested S-NSSAI;

c) optionally a requested DNN;

d) optionally the requested application requirements containing:

1) time window;

2) location criteria;

3) access type preference; and

4) UE IP address preservation indicator; and

e) optionally a requested configuration cause,

for a specific VAL service identified by a VAL service ID, toward a SNSCE-S to perform a network triggered slice configuration for the list of one or more VAL UEs for that specific VAL service.

NOTE: In this release, S-NSSAI and DNN are the only used route selection descriptors of the URSP rules described in 3GPP TS 24.526 [3].

B.2.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/su_nsc/<apiVersion>/val-services/{valServiceId}/configurations/{configurationId}**

This resource shall support the resource URI variables defined in the table B.2.1.2.2.2-1.

Table B.2.1.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause B.1.1
apiVersion	string	See clause B.2.1.1
valServiceId	string	Identifier of a VAL service.
configurationId	string	Identifier of a configuration

B.2.1.2.2.3 Resource Standard Method

B.2.1.2.2.3.1 PUT

This operation is to update a given configuration for one or more VAL UEs for a given VAL service which is provided by the SNSCE-S.

This method shall support the request data structures specified in table B.2.1.2.2.3.1-1, the response data structures and response codes specified in table B.2.1.2.2.3.1-2.

Table B.2.1.2.2.3.1-1: Data structures supported by the PUT Request payload on this resource

Attribute name	Data type	P	Cardinality	Description	Applicability
VAL UE List	array(string)	M	1..N	Represents a space-separated of VAL UE IDs within a given VAL service, for which a given network slice configuration trigger applies. The VAL service is identified by the value "valServiceId" and the network slice configuration is identified by the value "configurationId".	
Requested S-NSSAI	string	M	1	The new S-NSSAI which is requested.	
Requested DNN	string	O	0..1	The new DNN which is requested.	
request application requirements	ApplicationRequirements	O	0..1	The application-related request parameters.	
configuration cause	string	O	0..1	Indicates the cause for the configuration.	

Table B.2.1.2.2.3.1-1A: Definition of the ApplicationRequirements data type

Attribute name	Data type	P	Cardinality	Description
timeWindows	array(TimeWindow)	O	1..N	Indication of the new scheduled time window that is requested.
locationCriteria	UserLocation	O	0..1	Indication of the new location criteria that is requested. The data type of the LocationCriteria is UserLocation as specified in 3GPP TS 29.571[14].
accessTypePreference	string	O	0..1	Indication of the new access type (3GPP, non-3GPP or multi-access) preference that is requested.
uEIPaddressPreservationIndicator	boolean	O	0..1	Indication that UE IP address preservation is requested. Indicates whether UE IP address preservation is requested: - true(default): requested - false: not requested

Table B.2.1.2.2.3.1-1B: Definition of the TimeWindow data type

Attribute name	Data type	P	Cardinality	Description
startTime	DateTime	M	1	The data type of the start time field is DataTime as specified in 3GPP TS 29.571[14].
stopTime	DateTime	M	1	The data type of the stop time field is DataTime as specified in 3GPP TS 29.571[14].

Table B.2.1.2.2.3.1-2: Data structures supported by the PUT Response payload on this resource

Data type	P	Cardinality	Response Codes (NOTE)	Description
n/a			2.04 Changed	The configuration of the VAL UEs with VAL UE List within the VAL service identified by the value "valServiceId" and for the network slice configuration identified by the value "configurationId, was successful.
NOTE: The mandatory CoAP error status codes for the PUT method listed in table B.1.3-1 shall also apply.				

B.2.1.3 Error Handling

General error responses are defined in clause B.1.3.

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2021-08	CT1#131-e	C1-214994				TS skeleton for Network slice capability management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification	0.0.0
2021-08	CT1#131-e	C1-214983				Network slice capability management procedures	0.1.0
2021-08	CT1#131-e	C1-214993				Requirements for functional entities	0.1.0
2021-10	CT1#132-e	C1-216124				Correction of event triggered network slice adaptation procedure	0.2.0
2021-12	CT#94e					Creation of version 1.0.0 for CT#94 for information	1.0.0
2022-01	CT1#133-bis-e	C1-220187				Definitions of terms and symbols for network slice capability enablement Spec.	1.1.0
2022-01	CT1#133	C1-220578				Network slice adaptation	1.1.0
2022-01	CT1#133	C1-220579				Resolving EN	1.1.0
2022-01	CT1#133	C1-220580				General description for network slice capability enablement Spec	1.1.0
2022-01	CT1#133	C1-220581				Scope for network slice capability enablement Spec	1.1.0
2022-01	CT1#133	C1-220618				Replace management with enablement	1.1.0
2022-02	CT1#134	C1-221253				Clarification on route selection descriptors	1.2.0
2022-03	CT1#95e	CP-220315				Specification presented for approval, v2.0.0	2.0.0
2022-03	CT#95e					TS 24.549 v17.0.0 created after CT#95e by MCC	17.0.0
2022-06	CT#96	CP-221217	0001	2	B	Authenticate of SNSCE-C identity	17.1.0
2022-06	CT#96	CP-221217	0002	3	B	CoAP encoding	17.1.0
2022-06	CT#96	CP-221217	0003	2	B	CoAP requirements for SNSCE-C	17.1.0
2022-06	CT#96	CP-221217	0004	1	B	CoAP requirements for SNSCE-S	17.1.0
2022-06	CT#96	CP-221217	0005	1	F	Re-order the reference	17.1.0
2022-06	CT#96	CP-221217	0006	2	B	SNSCE client CoAP procedure	17.1.0
2022-06	CT#96	CP-221217	0007	3	B	SNSCE server CoAP procedure	17.1.0
2022-06	CT#96	CP-221217	0008	1	F	HTTP parameters	17.1.0
2022-06	CT#96	CP-221217	0009	1	F	Modification of general descriptions	17.1.0
2022-06	CT#96	CP-221217	0010	1	F	SNSCE client HTTP procedure	17.1.0
2022-06	CT#96	CP-221217	0011	1	F	SNSCE server HTTP procedure	17.1.0
2022-09	CT#97e	CP-222150	0012	1	F	Added description and overview	17.2.0
2023-03	CT#99	CP-230233	0013		F	Requirements alignment and miscellaneous corrections	17.3.0
2023-12	CT#102	CP-233190	0015	2	F	Update to the obsoleted IETF HTTP RFCs	18.0.0
2024-03	CT#103	CP-240118	0016	1	B	Update the general description	18.1.0
2024-03	CT#103	CP-240118	0017	1	B	Add parameters to network slice adaptation trigger	18.1.0
2024-03	CT#103	CP-240118	0018	2	B	Update APIs for event triggered network slice configuration	18.1.0
2024-03	CT#103	CP-240118	0019	2	B	Retrieve data and information from NSCE client	18.1.0
2024-03	CT#103	CP-240118	0020	2	B	Notify slice modification in Inter-PLMN based slice service continuity	18.1.0

History

Document history		
V18.1.0	May 2024	Publication