

ETSI TS 124 549 V17.0.0 (2022-05)



5G;
Network slice capability enablement-
Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification;
Stage 3
(3GPP TS 24.549 version 17.0.0 Release 17)



Reference

RTS/TSGC-0124549vh00

Keywords

5G

ETSI

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

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

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

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

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

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

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

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

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

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

Copyright Notification

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

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

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

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	4
1 Scope	6
2 References	6
3 Definitions of terms, symbols and abbreviations	6
3.1 Terms.....	6
3.2 Abbreviations	7
4 General description.....	7
5 Functional entities	8
5.1 SEAL network slice capability enablement client (SNSCE-C).....	8
5.2 SEAL network slice capability enablement server (SNSCE-S)	8
6 Network slice capability enablement procedures	8
6.1 General	8
6.2 On-network procedures	8
6.2.1 General.....	8
6.2.1.1 Authenticated identity in HTTP request.....	8
6.2.2 Event triggered network slice adaptation.....	9
6.2.2.1 General	9
6.2.2.2 Client procedure	9
6.2.2.3 Server procedure	9
6.3 Off-network procedures	10
Annex <A> (normative): Parameters for different operations.....	11
A.1 Event triggered network slice adaptation	11
A.1.1 General	11
A.1.2 Client side parameters	11
Annex (informative): <Informative annex for a Technical Specification>.....	12
B.1 Heading levels in an annex.....	12
Annex <C> (informative): Change history	13
History	14

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. 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].

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;".
- [3] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".
- [4] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification;".
- [5] OMA OMA-TS-XDM_Group-V1_1_1-20170124-A: "Group XDM Specification".
- [6] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".
- [7] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".
- [8] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".
- [9] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".
- [10] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

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

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
PCF	Policy Control Function
SEAL	Service Enabler Architecture Layer
SNSCE-C	SEAL Network Slice Capability Enablement Client
SNSCE-S	SEAL Network Slice Capability EnablementServer
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 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 OMA OMA-TS-XDM_Group-V1_1_1-20170124-A [5]; and
- c) shall support S-NSSAI and DNN adaptation due to new requirements or change of requirements for one or more application.

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 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_Group-V1_1_1-20170124-A [5]; and
- c) shall provide the 5GC network a guidance for route selection descriptors to assign new S-NSSAI and DNN.

6 Network slice capability enablement procedures

6.1 General

The network slice capability enablement procedures is a SEAL service providing capabilities for network slice re-mapping from one VAL application to one or more other VAL applications, 3GPP TS 23.434 [2]. 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.

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

6.2 On-network procedures

6.2.1 General

6.2.1.1 Authenticated identity in HTTP request

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

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 adaptation is sent by the client to the server. The network slice adaptation request may be sent by a VAL server for the adaptation of the network slice to the VAL application. The network slice adaptation request may be sent by the SNSCE-C acting as application client requesting for a new slice enablement.

NOTE: The interaction between VAL server and SNSCE-S is out of scope of this specification.

6.2.2.2 Client procedure

In order to request for network slice adaptation, the SNSCE-C shall send an HTTP POST request message according to procedures specified in IETF RFC 7231 [7]. In the HTTP POST 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-C appended with VAL service identity and the value "/UE-triggered-slice-adaptation";
- 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 [8];
- d) shall include the parameters for VAL UE list and requested S-NSSAI as specified in table A.1.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [9]; and
- e) may include the parameters for requested DNN and slice adaptation cause as specified in table A.1.2-1 of annex A serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 8259 [9].

6.2.2.3 Server procedure

Upon receipt an HTTP POST request from the SNSCE-C for network slice adaptation, the SNSCE-S shall determine the identity of the sender 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 slice 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 and slice adaptation cause from the HTTP POST 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 [10].

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

- 2) shall send the updated network slice and any new 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 or failure status of the requested network slice adaptation to the SNSCE-C.

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): Parameters for different operations

A.1 Event triggered network slice adaptation

A.1.1 General

The information in this annex provides a normative description for the parameters which are used by the SNSCE-C to trigger a network slice adaptation for a VAL application by sending to the SNSCE-S.

A.1.2 Client side parameters

The SNSCE-C uses the parameters shown in table A.1.2-1 to trigger network slice adaptation for a VAL application.

Table A.1.2-1: Client side parameters for network slice adaptation trigger

Parameter	Description
VAL UE List	REQUIRED. Represents a space-separated list of VAL UE Ids within the VAL service, for which the network slice adaptation trigger applies.
VAL service ID	REQUIRED. The VAL service ID of the VAL application
Requested S-NSSAI	REQUIRED. The new S-NSSAI which is requested
Requested DNN	OPTIONAL. The new DNN which is requested
Slice adaptation cause	OPTIONAL. Indicates the cause for the slice adaptation.

Annex (informative): <Informative annex for a Technical Specification>

B.1 Heading levels in an annex

Heading levels within an annex are used as in the main document, but for Heading level selection, the "A.", "B.", etc. are ignored. e.g. **B.1.2** is formatted using *Heading 2* style.

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	CT1#95e					TS 24.549 v17.0.0 created after CT#95e by MCC	17.0.0

History

Document history		
V17.0.0	May 2022	Publication