|  |  |
| --- | --- |
| 3GPP TS 24.549 V0.2.0 (2021-10) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  Network slice capability management - Service Enabler Architecture Layer for Verticals (SEAL);  Protocol specification;  Stage 3  (Release 17) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 General description 7

5 Functional entities 7

5.1 SEAL network slice capability management client (SNSCM-C) 7

5.2 SEAL network slice capability management server (SNSCM-S) 7

6 Network slice capability management 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 8

6.2.2.1 General 8

6.2.2.2 Client procedure 8

6.2.2.3 Server procedure 9

6.3 Off-network procedures 9

Annex <A> (normative): Parameters for different operations 9

A.1 Event triggered network slice adaptation 9

A.1.1 General 9

A.1.2 Client side parameters 9

Annex <B> (informative): <Informative annex for a Technical Specification> 10

B.1 Heading levels in an annex 10

Annex <X> (informative): Change history 11

# 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

This clause shall start on a new page.

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".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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].

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

## 3.3 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

DNN Data Network Name

HTTP Hypertext Transfer Protocol

PCF Policy Control Function

SEAL Service Enabler Architecture Layer

SNSCM-C SEAL Network Slice Capability Management Client

SNSCM-S SEAL Network Slice Capability Management Server

S-NSSAI Single Network Slice Selection Assistance Information

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

General description on network slice capability management and its protocol

# 5 Functional entities

## 5.1 SEAL network slice capability management client (SNSCM-C)

The SNSCM-C functional entity acts as the application client for managing network slice capabilities. To be compliant with the procedures in the present document the SNRM-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 management server (SNSCM-S)

The SNSCM-S is a functional entity which provides slice capability management to administer the network slice for one or more vertical applications. To be compliant with the procedures in the present document the SNSCM-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 management procedures

## 6.1 General

The network slice capability management 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.

## 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 SNSCM-C, the SNSCM-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 SNSCM-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 subclauses 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 SNSCM-C acting as application client requesting for a new slice enablement.

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

#### 6.2.2.2 Client procedure

In order to request for network slice adaptation, the SNSCM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 7231 [7]. In the HTTP POST request message, the SNSCM-C:

a) shall set the Request-URI to the URI identifying the SNSCM-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 SNSCM-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 SNSCM-C for network slice adaptation, the SNSCM-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 SNSCM-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 SNSCM-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 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;

Editor's note: How the SNSCM-S updates the network slice for one or more VAL UEs for a VAL service, needs to be specified.

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 SNSCM-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 SNSCM-C to trigger a network slice adaptation for a VAL application by sending to the SNSCM-S.

## A.1.2 Client side parameters

The SNSCM-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 <B> (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 <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-08 | CT1#131-e | [C1-214994](https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_131e/Docs/C1-214994.zip) |  |  |  | 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](https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_131e/Docs/C1-214983.zip) |  |  |  | Network slice capability management procedures | 0.0.0 |
| 2021-08 | CT1#131-e | [C1-214993](https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_131e/Docs/C1-214993.zip) |  |  |  | Requirements for functional entities | 0.0.0 |