ETSI TS 124 546 V19.3.0 (2026-03)

TECHNICAL SPECIFICATION

5G;
Configuration management - Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification
(3GPP TS 24.546 version 19.3.0 Release 19)

Reference
RTS/TSGC-0124546vj30

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 IPR online database.

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

Trademarks

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

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

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

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

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

Contents

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 for the configuration management capability of SEAL to support vertical applications (e.g. V2X) over the 3GPP system.

The present document is applicable to the User Equipment (UE) supporting the configuration management client functionality as described in 3GPP TS 23.434 [2], to the application server supporting the configuration management server functionality as described in 3GPP TS 23.434 [2] and to the application server supporting the vertical application server (VAL server) functionality as defined in specific vertical application service (VAL service) specification.

NOTE: The specification of the VAL server for a specific VAL service is out of scope for 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] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

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

[5] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

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

[7] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

[8] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[9] IETF RFC 5875: "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".

[10] IETF RFC 6050: "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[11] IETF RFC 6665: "SIP-Specific Event Notification".

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

[13] IETF RFC 7959: "Block-Wise Transfers in the Constrained Application Protocol (CoAP)".

[14] IETF RFC 7641: "Observing Resources in the Constrained Application Protocol (CoAP)".

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

[16] void

[17] IETF RFC 8949: "Concise Binary Object Representation (CBOR)".

[18] IETF RFC 8610: "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures".

[19] Constrained RESTful Environments (CoRE) Parameters at IANA, https://www.iana.org/assignments/core-parameters/core-parameters.xhtml

[20] IETF RFC 9290: "Concise Problem Details for Constrained Application Protocol (CoAP) APIs".

[21] IETF RFC 9177: "Constrained Application Protocol (CoAP) Block-Wise Transfer Options Supporting Robust Transmission".

[22] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[23] 3GPP TS 29.501: "Principles and Guidelines for Services Definition".

[24] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[25] IETF RFC 3339: "Date and Time on the Internet: Timestamps".

[26] 3GPP TS 23.003: "Numbering, addressing and identification".

[27] Void

[28] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[29] 3GPP TS 29.572: "5G System; Location Management Services; Stage 3".

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

[31] 3GPP TS 29.122: "T8 reference point for northbound Application Programming Interfaces (APIs)".

[32] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[33] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

3 Definitions of terms 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 configuration management client: An entity that provides the client side functionalities corresponding to the SEAL configuration management service.

SEAL configuration management server: An entity that provides the server side functionalities corresponding to the SEAL configuration management 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].

MIME	Multipurpose Internet Mail Extensions
SCM-C	SEAL Configuration Management Client
SCM-S	SEAL Configuration Management Server
SEAL	Service Enabler Architecture Layer for verticals

4 General description

Configuration management is a SEAL service that provides the configuration management related capabilities to one or more vertical applications. The present document enables a SEAL configuration management client (SCM-C) and a VAL server to manage configuration data in a SEAL configuration management server (SCM-S).

5 Functional entities

5.1 SEAL configuration management client (SCM-C)

The SCM-C functional entity acts as the application client for configuration related transactions.

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

- shall support the role of XCAP client as specified in IETF RFC 4825 [3];
- shall support the role of XDMC as specified in OMA OMA-TS-XDM_Core-V2_1 [4];
- shall support the procedures in clause 6.2.2;
- shall support the procedures in clause 6.2.3;
- shall support the procedures in clause 6.2.4;and
- shall support the procedures in clause 6.2.5.

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

- shall support the role of CoAP client as specified in IETF RFC 7252 [12];
- shall support the capability to observe resources as specified in IETF RFC 7641 [14];
- shall support the block-wise transfer as specified in IETF RFC 7959 [13];
- may support the robust block transfer as specified in IETF RFC 9177 [21];
- should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [15];
- shall support CBOR encoding as specified in IETF RFC 8949 [17];
- shall support the procedures in clause 6.2.2;
- shall support the procedures in clause 6.2.3;
- shall support the procedures in clause 6.2.4;and
- shall support the procedures in clause 6.2.5

NOTE 1: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [5].

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.

NOTE 3: The CoAP protocol supports mechanism for reliable message exchange over UDP. Use of TCP can also be beneficial if reliable transport is required for other reasons, e.g. better observability of resources. Usage of CoAP over TCP is an implementation choice.

NOTE 4: Support for the robust block transfer mechanism for the CoAP procedures is beneficial in environments where packet loss is highly asymmetrical and where performance optimization of block transfers is required.

5.2 SEAL configuration management server (SCM-S)

The SCM-S is a functional entity used to configure one or more vertical applications with 3GPP system related vertical applications provisioning information and configure data on the SEAL configuration management client.

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

- shall support the role of XCAP server as specified in IETF RFC 4825 [3];
- shall support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [4];
- shall support the procedures in clause 6.2.2;
- shall support the procedures in clause 6.2.3;
- shall support the procedures in clause 6.2.4;
- shall support the procedures in clause 6.2.5.

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

- shall support the role of CoAP server as specified in IETF RFC 7252 [12];
- shall support the capability to observer resources as specified in IETF RFC 7641 [14];
- shall support the block-wise transfer as specified in IETF RFC 7959 [13];
- shall support the robust block transfer as specified in IETF RFC 9177 [21];
- shall support CoAP over TCP and Websocket as specified in IETF RFC 8323 [15];
- shall support CBOR encoding as specified in IETF RFC 8949 [17];
- shall support the procedures in clause 6.2.2;
- shall support the procedures in clause 6.2.3;
- shall support the procedures in clause 6.2.4;and
- shall support the procedures in clause 6.2.5.

NOTE: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [5]

6 Configuration management procedures

6.1 General

6.2 On-network procedures

6.2.1 General

6.2.1.1 Authenticated identity in HTTP request

Upon receiving an HTTP request, the SCM-S shall authenticate the identity of the sender of the HTTP request as specified in 3GPP TS 24.547 [5], and if authentication is successful, the SCM-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 an CoAP request, the SCM-S shall authenticate the identity of the sender of the CoAP request as specified in 3GPP TS 24.547 [5], and if authentication is successful, the SCM-S shall use the identity of the sender of the CoAP request as an authenticated identity.

6.2.2 Common procedures

6.2.2.1 Management of configuration update event subscription

6.2.2.1.1 SIP based procedures

6.2.2.1.1.1 General

The VAL service will use the same identity which has been authenticated by VAL service with SIP core using SIP based REGISTER message. If VAL service do not support SIP protocol, then HTTP based method needs to be used.

The SCM-C shall use mechanism provided by VAL service to add access-token in SIP messages. The SCM-S shall identify the originating VAL user ID from the access-token received from SCM-C using the mechanism defined in VAL service specification.

6.2.2.1.1.2 Create subscription

In order to subscribe to notification of changes of one or more group documents of VAL groups identified by VAL group IDs, a SCM-C shall send an initial SIP SUBSCRIBE request to the network according to the UE originating procedures specified in 3GPP TS 24.229 [8] and IETF RFC 5875 [9]. In the initial SIP SUBSCRIBE request, the SCM-C:

a) shall set the Request-URI to the configured public service identity for performing subscription proxy function of the SCM-S;

b) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.seal" (coded as specified in 3GPP TS 24.229 [8]), in a P-Preferred-Service header field according to IETF RFC 6050 [10];

c) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.seal" in the Contact header field;

d) shall include an application/resource-lists+xml MIME body. In the application/resource-lists+xml MIME body, the SCM-C shall include one <entry> element for each configuration document to be subscribed to, such that the "uri" attribute of the <entry> element contains a relative path reference to XCAP URI identifying an XML document to be subscribed to;and

e) if the VAL server wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [11], to zero. Otherwise, shall set the Expires header field to the duration for which VAL user has requested for subscription.

Upon reception of an initial SIP SUBSCRIBE request:

a) with the Event header field set to xcap-diff;

b) with the Request-URI set to own public service identity for performing subscription proxy function of the SCM-S;

c) with an application/resource-lists+xml MIME body; and

d) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.seal" (coded as specified in 3GPP TS 24 229 [8]), in a P-Asserted-Service header field according to IETF RFC 6050 [10];

the SCM-S:

a) shall identify the originating VAL user ID and shall use the originating VAL user ID as an authenticated identity when performing the authorization;

b) if the authenticated identity is not authorized to subscribe to notification of changes of any resource in the application/resource-lists+xml MIME body, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps;and

c) act as a notifier according to IETF RFC 5875 [9].

6.2.2.1.1.3 Modify subscription

In order to modify or refresh subscription, the SCM-C shall send SIP re-SUBSCRIBE request on the same dialog as the existing subscription, and with the same "Event" header. The SCM-C shall follow the steps specified in clause 6.2.2.1.1.2 to create SIP SUBSCRIBE request.

Upon reception of a SIP re-SUBSCRIBE request:

a) with the Event header field set to xcap-diff; and

b) with an application/resource-lists+xml MIME body;

the SCM-S:

a) act as a notifier according to IETF RFC 5875 [9].

6.2.2.1.1.4 Delete subscription

In order to delete the subscription, the SCM-C shall send SIP re-SUBSCRIBE request on the same dialog as the existing subscription, and with the same "Event" header. The SCM-C shall follow the steps specified in clause 6.2.2.1.1.2 to create SIP SUBSCRIBE request with following clarification:

a) shall set the Expires header field to zero.

Upon reception of a SIP re-SUBSCRIBE request:

a) with the Event header field set to xcap-diff; and

b) with Expires header field set to zero;

the SCM-S:

a) act as a notifier according to IETF RFC 5875 [9].