ETSI TS 124 548 V17.6.0 (2025-03)

5G;
Network Resource Management -
Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification
(3GPP TS 24.548 version 17.6.0 Release 17)

Reference
RTS/TSGC-0124548vh60

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 network resource 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 network resource management client functionality as described in 3GPP TS 23.434 [2], to the application server supporting the network resource 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 the specific vertical application service (VAL service) specifications.

NOTE: The specification of the VAL server for a specific VAL service is out of scope of 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 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.203: "Policy and charging control architecture".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[7] 3GPP TS 24.486: "Vehicle-to-Everything (V2X) Application Enabler (VAE) layer; Protocol aspects; Stage 3".

[8] 3GPP TS 24.545: "Location Management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[9] 3GPP TS 24.547: "Identity management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[10] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[12] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[13] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point; Stage 3".

[14] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[15] Void.

[16] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed".

[17] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[18] IETF RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)".

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

[20] IETF RFC 5795: "The Robust Header Compression (ROHC) Framework".

[21] Void

[21A] IETF RFC 6838: "Media Type Specifications and Registration Procedures".

[22] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

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

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

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

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

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

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

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

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

[31] 3GPP TS 24.546: "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification".

[32] OMA OMA-TS-XDM_Core-V2_1-20120403-A: "XML Document Management (XDM) 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 network resource management client: An entity that provides the client side functionalities corresponding to the SEAL network resource management service.

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

BM-SC	Broadcast-Multicast Service Centre
SNRM-C	SEAL Network Resource Management Client
SNRM-S	SEAL Network Resource Management Server
PCF	Policy Control Function
SEAL	Service Enabler Architecture Layer for verticals
VAL	Vertical Application Layer

4 General description

Network resource management is a SEAL service that provides the network resource management related capabilities (e.g. unicast and multicast network resources) to one or more vertical applications. The present document enables a SEAL network resource management client (SNRM-C) and a VAL server that communicate with a SEAL network resource management server (SNRM-S).

The SNRM-S obtains and controls multicast resources from the underlying 3GPP network system via the BM-SC and controls unicast resources from the underlying 3GPP network system via the PCRF/PCF.

5 Functional entities

5.1 SEAL network resource management client (SNRM-C)

The SNRM-C functional entity acts as the application client for network resource management related transactions.

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

a) shall support the role of XCAP client as specified in IETF RFC 4825 [19];

b) shall support the role of XDMC as specified in OMA OMA-TS-XDM_Core-V2_1 [32]; and

c) shall support the multicast resource management procedures in clause 6.2.3.

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

- shall support the role of CoAP client as specified in IETF RFC 7252 [23];
- shall support the capability to observe resources as specified in IETF RFC 7641 [25];
- shall support the block-wise transfer as specified in IETF RFC 7959 [24];
- may support the robust block transfer as specified in IETF RFC 9177 [29];
- should support CoAP over TCP and Websocket as specified in IETF RFC 8323 [26];
- shall support CBOR encoding as specified in IETF RFC 8949 [27];
- shall support the procedures in clause 6.2.3; and

- shall support the procedure in clause 6.2.4.

NOTE 1: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [9].

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 network resource management SEAL server (SNRM-S)

The SNRM-S is a functional entity used to provide resource management of 3GPP system network resources (e.g. unicast, multicast) to one or more vertical applications.

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

a) shall support the role of XCAP server as specified in IETF RFC 4825 [19];

b) shall support the role of XDMS as specified in OMA OMA-TS-XDM_Core-V2_1 [32];

c) shall support the unicast resource management procedures in clause 6.2.2; and

d) shall support the multicast resource management procedures in clause 6.2.3.

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

- shall support the role of CoAP server as specified in IETF RFC 7252 [23];
- shall support the capability to observe resources as specified in IETF RFC 7641 [25];
- shall support the block-wise transfer as specified in IETF RFC 7959 [24];
- shall support the robust block transfer as specified in IETF RFC 9177 [29];
- shall support CoAP over TCP and Websocket as specified in IETF RFC 8323 [26];
- shall support CBOR encoding as specified in IETF RFC 8949 [27];
- shall support the procedure in clause 6.2.3; and
- shall support the procedure in clause 6.2.4.

NOTE: The security mechanism to be supported for the CoAP procedures is described in 3GPP TS 24.547 [9].

6 Network resource 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 SNRM-S shall authenticate the identity of the sender of the HTTP request is authorized as specified in 3GPP TS 24.547 [9], and if authentication is successful, the SNRM-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 SNRM-S shall authenticate the identity of the sender of the CoAP request as specified in 3GPP TS 24.547 [9], and if authentication is successful, the SNRM-S shall use the identity of the sender of the CoAP request as an authenticated identity.

6.2.2 Unicast resource management

6.2.2.1 General

This clause describes the procedures used for unicast resource management. The unicast resource management comprises procedures for:

a) activation and deactivation of bearers;

b) modification of the QoS characteristics of a bearer; and

c) modification of GBR due to application requirement.

The VAL client can request the VAL server to provide unicast resources (see clause 6.2.2.2), to modify or to release unicast resources (see clause 6.2.2.3) or to perform network resource adaptation (see clause 6.2.2.4).

NOTE: A VAL service communication can consist of both unicast and multicast bearers which can all need modification due to the same event.

VAL specific pre-requisites and resultant behaviour by functional entities in performing the unicast resource management procedures are specified in the respective VAL TS (e.g. for V2X application layer, see 3GPP TS 24.486 [7]).

Unicast resource management is supported with PCRF interactions with SIP core and PCC interactions with the SNRM-S. The PCRF procedures are specified in 3GPP TS 29.214 [12] and the PCF procedures are specified in 3GPP TS 29.514 [14].

6.2.2.2 Request for unicast resource at VAL service communication establishment procedure with SIP core

6.2.2.2.1 VAL server procedure

If the VAL client requests VAL service communication with the VAL server, the VAL server shall generate an HTTP POST request message according to procedures specified in IETF RFC 7231 [22]. In the HTTP POST request message, the VAL server:

a) shall include a Request-URI set to the URI corresponding to the identity of the SNRM-S;