ETSI TS 124 546 V17.2.0 (2022-07)

TECHNICAL SPECIFICATION

5G; Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification (3GPP TS 24.546 version 17.2.0 Release 17)

Reference

RTS/TSGC-0124546vh20

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/CommiteeSupportStaff.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

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

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 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[11] IETF RFC 6665 (July 2012): "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] IETF RFC 8516: ""Too Many Requests" Response Code for the Constrained Application Protocol".

[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] Internet draft draft-ietf-core-problem-details-01: "Problem Details For CoAP APIs".

[21] Internet draft draft-ietf-core-new-block-14: "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".

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; and
- shall support the procedures in clause 6.2.4.

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 draft draft-ietf-core-new-block-14 [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; and
- shall support the procedures in clause 6.2.4.

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; and
- shall support the procedures in clause 6.2.4.

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 draft draft-ietf-core-new-block-14 [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; and
- shall support the procedures in clause 6.2.4.

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;

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:

d) 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;

e) 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 6.2.2.1.1.2.1 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 6.2.2.1.1.2.1 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].

6.2.2.1.2 HTTP based procedures

6.2.2.1.2.1 Creating subscription

Upon successful service authorization of the VAL service, the SCM-C shall create a subscription for configuration events by sending an HTTP POST request to the SCM-S. In the HTTP POST request, the SCM-C:

a) shall set the Request URI to the URI of the SCM-S appended with VAL service identity and the value "/configurationEventsSubscription";

b) shall include the Host header with public user identity of SCM-S;

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 [6]; and

c) include the parameters specified in clause A.1.2 serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 7159 [7].

Upon reception of an HTTP POST request from SCM-C where the Request-URI of the HTTP POST request contains "/configurationEventsSubscription", the SCM-S:

a) shall determine the identity of the sender of the received HTTP POST request as specified in clause 6.2.1.1, and:

    1) if the identity of the sender of the received HTTP POST request is not authorized user, shall respond with an HTTP 403 (Forbidden) response to the HTTP POST request and skip rest of the steps;

b) shall generate unique subscription identity and store the subscription details for the authorized user; and

c) shall send an HTTP 200 (OK) response including parameters specified in clause A.1.3.

6.2.2.1.2.2 Modify a subscription

Upon receiving a request from VAL user to modify existing subscription identified with unique subscription identity, the SCM-C:

a) shall generate an HTTP PUT request. In the HTTP PUT request:

   1) shall set the Request URI to the same Request URI used while creating subscription in clause 6.2.2.1.2.1.1 appended with subscription identity;

   2) shall include the Host header with public user identity of SCM-S;

   3) 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 [6]; and

   4) include the parameters specified in clause A.1.2 serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 7159 [7].

b) shall send the HTTP PUT request to the SCM-S.

Upon reception of an HTTP PUT request from SCM-C where the Request-URI of the HTTP PUT request contains "/configurationEventsSubscription" appended with subscription identity, the SCM-S:

a) shall determine the identity of the sender of the received HTTP PUT request as specified in clause 6.2.1.1, and:

   1) if the identity of the sender of the received HTTP PUT request is not authorized user, shall respond with an HTTP 403 (Forbidden) response to the HTTP PUT request and skip rest of the steps;

b) shall determine whether subscription for configuration events exists or not based on received subscription identity in request URI; and

   1) if subscription does not exist, shall respond with an HTTP 406 (Not Acceptable) response to the HTTP PUT request and skip rest of the steps;

c) shall update the subscription details based on received parameters from the HTTP PUT request; and

d) shall send an HTTP 200 (OK) response including parameters specified in clause A.1.3.

6.2.2.1.2.3 Delete a subscription

Upon receiving a request from VAL user to delete existing subscription identified with unique subscription identity, the SCM-C:

a) shall generate an HTTP DELETE request. In the HTTP DELETE request:

   1) shall set the Request URI to the same Request URI used while creating subscription in clause 6.2.2.1.2.1.1 appended with subscription identity;

   2) shall include the Host header with public user identity of SCM-S; and

   3) 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 [6]; and

b) shall send the HTTP DELETE request to the SCM-S.

Upon reception of an HTTP DELETE request from SCM-C where the Request-URI of the HTTP DELETE request contains "/configurationEventsSubscription" appended with subscription identity, the SCM-S:

a) shall determine the identity of the sender of the received HTTP DELETE request as specified in clause 6.2.1.1, and:

   1) if the identity of the sender of the received HTTP DELETE request is not authorized user, shall respond with an HTTP 403 (Forbidden) response to the HTTP DELETE request and skip rest of the steps;

b) shall determine whether subscription for configuration events exists or not based on received subscription identity in request URI; and

   1) if subscription does not exist, shall respond with an HTTP 406 (Not Acceptable) response to the HTTP DELETE request and skip rest of the steps;

c) shall delete the subscription details based on received parameters from the HTTP DELETE request; and

d) shall send an HTTP 200 (OK) response to the SCM-C.

6.2.2.1.3 CoAP based procedures

6.2.2.1.3.1 General

CoAP based procedures shall use the mechanisms to observe a resource as specified in IETF RFC 7641 [14].

NOTE: CoAP "observe" mechanism uses the principle of eventual consistency where an intermediate state change can be lost when UDP is used. If it is critical for the client to receive every change in the resource state (and not just the latest state), TCP can be used to avoid missing notifications.

6.2.2.1.3.2 Create a subscription

In order to subscribe to changes of a configuration document the SCM-C shall send an extended CoAP GET request with the CoAP URI set to the URI of an observable configuration document and with the Observe option set to 0 (Register) as specified in IETF RFC 7641 [14].

Upon reception of such an extended CoAP request from SCM-C where the CoAP URI of the request points at an observable configuration document and with the Observe option set to 0 (Register), the SCM-S:

a) shall perform the steps as for a normal CoAP GET request for a configuration document as defined in clause 6.2.4.4 for VAL UE configuration and in clause 6.2.4.4 for VAL user profile;

b) shall register the SCM-C as an observer as per IETF RFC 7641 [14]; and

c) shall send a CoAP 2.05 (Content) response including the current content of the resource and the Observer option with the initial sequence number of the notifications.

6.2.2.1.3.3 Delete a subscription

In order to unsubscribe from changes of a configuration document the SCM-C shall send a CoAP GET request matching the CoAP GET request used to create the subscription but with the Observe option set to 1 (Deregister) as specified in IETF RFC 7641 [14].

Upon reception of a CoAP GET that matches an active subscription but with the Observe option set to 1 (Deregister), the SCM-S:

a) shall perform the steps as for a normal CoAP GET request for a configuration document as defined in clause 6.2.4.4 for VAL UE configuration and in clause 6.2.4.4 for VAL user profile;

b) shall deregister the SCM-C as an observer as per IETF RFC 7641 [14]; and

c) shall send a CoAP 2.05 (Content) response including the current content of the resource and shall not include the Observer option.

6.2.2.2 Notifications

6.2.2.2.1 SIP based procedures

6.2.2.2.1.1 Client procedure

Upon receiving a SIP NOTIFY request associated with a subscription created as result of the sent initial SIP SUBSCRIBE request, the SCM-S:

a) shall handle the SIP NOTIFY request according to IETF RFC 5875 [9].

6.2.2.2.1.2 Server procedure

In order to send notification of group document update event, the SCM-S shall send SIP NOTIFY to SCM-C according to IETF RFC 5875 [9].

6.2.2.2.2 HTTP based procedures

6.2.2.2.2.1 Receiving configuration update notification

Upon receiving an HTTP POST request over a call back URI which was given to SCM-S at time of the configuration update event subscription message, the SCM-C:

a) shall validate the subscription identity received in the "Identity" parameter of the HTTP POST request. If the subscription identity is not valid, the SCM-C:

   1) shall send an HTTP 406 (Not Acceptable) response and skip rest of the steps;

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

c) shall notify the VAL user about the modification of configuration document based on the "Event" parameter.

Based on VAL user's request, the SCM-C may also retrieve the configuration document as specified in clause 6.2.3 or in clause 6.2.4.

6.2.2.2.2.2 Sending group modify notification

Upon successful modification of VAL user profile document or VAL UE configuration document, the SCM-S sends a notification to SCM-C. The SCM-S:

a) shall check whether valid configuration update event subscription exists for event SUBSCRIBE_USER_PROFILE_MODIFICATION (0x01) OR SUBSCRIBE_UE_CONFIG_MODIFICATION (0x02) as defined in clause A.1.2 or not;

   1) if valid subscription does not exist, shall skip rest of the steps;

b) shall generate an HTTP POST message to notify configuration update notification. In HTTP POST message:

   1) shall set the request URI to call back URI received in the creating subscription procedure;

   2) shall set the Content-Type header to "application/json"; and

   3) shall include an HTTP request entity-body with the parameters specified in clause B.2 serialized into a JavaScript Object Notation (JSON) structure; and

c) shall sent an HTTP POST request towards SCM-C.

6.2.2.2.3 CoAP based procedures

6.2.2.2.3.1 Client procedure

Upon receiving a CoAP 2.05 (Content) response that matches the extended CoAP GET request which initiated the subscription and which contains the Observe option, the SCM-C:

a) shall handle the response according to IETF RFC 7641 [14]; and

b) shall notify the VAL user about the modification of the configuration document.

6.2.2.2.3.2 Server procedure

In order to send a notification when the configuration document is modified, the SCM-S shall send a CoAP 2.05 (Content) response to SCM-C containing the modified document and the Observe option according to IETF RFC 7641 [14]. The Content-Format specified in a 2.xx notification shall be the same as the one used in the initial response to the GET request received for the subscription.

6.2.3 VAL UE configuration data

6.2.3.1 SCM client HTTP procedure

Upon receiving a request from the VAL user to retrieve a VAL UE configuration data, the SCM-C shall send an HTTP GET request to the SCM-S according to procedures specified in IETF RFC 4825 [3] "*Fetch a Document*". In HTTP GET request, the SCM-C:

a) shall set the Request-URI to a XCAP URI identifying the XML document to be retrieved. In the Request-URI:

   1) the "XCAP Root" is set to the URI of the SCM-S;

   2) the "auid" is set to specific VAL service identity; and

   3) the document selector is set to a document URI pointing to the VAL UE configuration document;

b) 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 [6]; and

c) may include the parameters specified in clause A.2.1 serialized into a JavaScript Object Notation (JSON) structure as specified in IETF RFC 7159 [7]

6.2.3.2 SCM server HTTP procedure

Upon reception of an HTTP GET request where the Request-URI of the HTTP GET request identifies a UE configuration document as specified in the specific vertical application, the SCM-S:

a) shall determine the identity of the sender of the received HTTP GET request as specified in clause 6.2.1.1, and:

   1) if the identity of the sender of the received HTTP GET request is not authorized to fetch requested configuration document, shall respond with a HTTP 403 (Forbidden) response to the HTTP GET request and skip rest of the steps; and

b) shall support handling an HTTP GET request from a SCM-C according to procedures specified in IETF RFC 4825 [3] "*GET Handling*".

6.2.3.3 SCM client CoAP procedure

Upon receiving a request from the VAL user to retrieve a VAL UE configuration data, the SCM-C shall send a CoAP GET request to the SCM-S. In the CoAP GET request, the SCM-C:

a) shall set the CoAP URI identifying the user profile document to be retrieved according to the resource API definition in Annex C.4.1:

   1) the "apiRoot" is set to the SCM-S URI;

   2) the "valServiceId" is set to specific VAL service;

   3) if the SCM-C does not know the "ueConfigDocId" of the UE configuration document at the SGM-S, the SCM-C shall make a GET request for the UE Configurations as described in Annex C.4.1.2.2.3.1 and shall set applicable query parameters defined in table C.4.1.2.2.3.1-1; and

   4) if the SCM-C knows the "ueConfigDocId" of the UE configuration document at the SGM-S, the SCM-C shall make a GET request for the Individual UE Configuration as described in Annex C.4.1.2.3.3.1, and shall set "ueConfigDocId" to point to the VAL UE configuration document; and

b) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [5].

Editor's note: The method to protect the request will be decided by SA3, and necessary alignment with SA3 is FFS.

6.2.3.4 SCM server CoAP procedure

Upon reception of an CoAP GET request where the CoAP URI of the request identifies UE Configurations resource as described in Annex C.4.1.2.2.3.1, the SCM-S:

a) shall determine the identity of the sender of the received CoAP GET request as specified in clause 6.2.1.2, and:

   1) if the sender is not authorized to fetch the requested UE configuration document(s), shall respond with a CoAP 4.03 (Forbidden) response to the CoAP GET request and skip rest of the steps;

b) shall support handling a CoAP GET request from a SCM-C according to procedures specified in IETF RFC 7252 [12];

c) shall check if the resource exists for the given VAL service, and:

   1) if the resource does not exist, shall return a 4.04 (Not found) response and skip rest of the steps; and

d) shall return a 2.05 (Content) response including all the UE configuration documents found for the given values of the query parameters defined in table C.4.1.2.2.3.1-1.

Upon reception of an CoAP GET request where the CoAP URI of the request identifies Individual UE Configuration resource as described in Annex C.4.1.2.3.3.1, the SCM-S:

a) shall determine the identity of the sender of the received CoAP GET request as specified in clause 6.2.1.2, and:

   1) if the sender is not authorized to fetch the requested UE configuration document, shall respond with a CoAP 4.03 (Forbidden) response to the CoAP GET request and skip rest of the steps;

b) shall support handling a CoAP GET request from a SCM-C according to procedures specified in IETF RFC 7252 [12]; and

c) shall check if the resource pointed at by the CoAP URI exists and:

   1) if it exists, shall return the UE configuration document in a 2.05 (Content) response; or

2) otherwise, shall return a 4.04 (Not found) response.

6.2.4 VAL user profile data

6.2.4.1 SCM client HTTP procedure

Upon receiving a request from the VAL user to retrieve a VAL user profile data, the SCM-C shall send an HTTP GET request to the SCM-S according to procedures specified in IETF RFC 4825 [3] "*Fetch a Document*". In HTTP GET request, the SCM-C:

a) shall set the Request-URI to a XCAP URI identifying the XML document to be retrieved. In the Request-URI:

   1) the "XCAP Root" is set to the URI of the SCM-S;

   21) the "auid" is set to specific VAL service identity; and

   3) the document selector is set to a document URI pointing to the VAL user profile document; and

b) 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 [6].

6.2.4.2 SCM server HTTP procedure

Upon reception of an HTTP GET request where the Request-URI of the HTTP GET request identifies a user profile document as specified in the specific vertical application, the SCM-S follow the procedure as described in clause 6.2.3.2.

6.2.4.3 SCM client CoAP procedure

Upon receiving a request from the VAL user to retrieve a VAL user profile data, the SCM-C shall send a CoAP GET request to the SCM-S. In the CoAP GET request, the SCM-C:

a) shall set the CoAP URI identifying the user profile document to be retrieved according to the resource API definition in Annex C.2.1:

   1) the "apiRoot" is set to the SCM-S URI;

   2) the "valServiceId" is set to specific VAL service; and

   3) if the SCM-C does not know the "profileDocId" of the user profile document at the SGM-S, the SCM-C:

      i) shall use the User Profiles resource GET, as described in Annex C.2.1.2.2.3.1, and shall set val-tgt-ue to either the VAL user identity or VAL UE identity; or

      ii) shall use the Individual User Profile resource GET, as described in Annex C.2.1.2.3.3.1, and shall set "profileDocId" to point to the VAL user profile document; and

b) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [5].

Editor's note: The method to protect the request will be decided by SA3, and necessary alignment with SA3 is FFS.

6.2.4.4 SCM server CoAP procedure

Upon reception of an CoAP GET request where the CoAP URI of the request identifies User Profiles resource as described in Annex C.2.1.2.2.3.1, the SCM-S:

a) shall determine the identity of the sender of the received CoAP GET request as specified in clause 6.2.1.2, and:

   1) if the identity of the sender of the received CoAP GET request is not authorized to fetch requested user profile document(s), shall respond with a CoAP 4.03 (Forbidden) response to the CoAP GET request and skip rest of the steps;

b) shall support handling a CoAP GET request from a SCM-C according to procedures specified in IETF RFC 7252 [12]; and

c) shall check if the resource exists for the given VAL service, and:

   1) if the resource does not exist, shall return a 4.04 (Not found) response and skip rest of the steps;

d) shall return a 2.05 (Content) response including all the user profile documents found for the given VAL user or VAL UE given in the query parameter.

Upon reception of an CoAP GET request where the CoAP URI of the request identifies Individual User Profile resource as described in Annex C.2.1.2.3.3.1, the SCM-S:

a) shall determine the identity of the sender of the received CoAP GET request as specified in clause 6.2.1.2, and:

   1) if the identity of the sender of the received CoAP GET request is not authorized to fetch requested user profile document, shall respond with a CoAP 4.03 (Forbidden) response to the CoAP GET request and skip rest of the steps;

b) shall support handling a CoAP GET request from a SCM-C according to procedures specified in IETF RFC 7252 [12]; and

c) shall check if the resource pointed at by the CoAP URI exists and:

   1) if it exists, shall return the user profile document in the 2.05 (Content) response; or

   2) otherwise, shall return a 4.04 (Not found) response.

6.2.5 Update VAL user profile data

6.2.5.1 SCM client HTTP procedure

Upon receiving a request from the VAL user to update the VAL user profile configuration document, the SCM-C shall create an XML document as specified in coding of the specific vertical application and shall send the XML document to the SCM-S according to procedures specified in IETF RFC 4825 [3] "*Create or Replace a Document*". In the HTTP POST request, the SCM-C:

a) shall set the Request URI to a XCAP URI identifying an XML document to be updated. In the Request-URI:

   1) the "XCAP Root" is set to the URI of the SCM-S;

   2) the "auid" is set to specific VAL service identity; and

   3) the document selector is set to the VAL user profile;

b) 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 [6];

c) shall include a Content-Type header field set to "application/vnd.3gpp.seal-user-profile-info+xml"; and

d) shall include an application/vnd.3gpp.seal-user-profile-info+xml MIME body and in the <seal-user-profile> root element:

   1) may include <ProfileName> element indicating name of the profile;

   2) may include <Status> element indicating status of the profile;

   3) may include <isDefault> element indicating that the current profile is the selected profile for the requesting user;

   4) shall include <user-profile-index> element indicating the unique profile number; and

   5) shall include <profile-configuration> element as specified in clause 7.

6.2.5.2 SCM server HTTP procedure

Upon reception of an HTTP PUT request where the Request-URI of the HTTP PUT request identifies an XML document as specified in the specific vertical application, the SCM-S:

a) shall determine the identity of the sender of the received HTTP PUT request as specified in clause 6.2.1.1, and:

   1) if the identity of the sender of the received HTTP PUT request is not authorized to update the configuration document, shall respond with a HTTP 403 (Forbidden) response to the HTTP PUT request and skip rest of the steps; and

b) shall support receiving an XML document as specified in application usage of the specific vertical application according to procedures specified in IETF RFC 4825 [3] "*PUT Handling*".

6.2.5.3 SCM client CoAP procedure

Upon receiving a request from the VAL user to update the VAL user profile configuration document, the SCM-C shall send a CoAP PUT request to the SCM-S. In the CoAP PUT request, the SCM-C:

a) shall set the CoAP URI identifying the user profile document to be updated according to the resource definition in Annex C.2.1.2.3.3.2:

   1) the "apiRoot" is set to the SCM-S URI;

   2) the "valServiceId" is set to specific VAL service; and

   3) the "profileDocId" to point to the VAL user profile document;

b) shall include Content-Format option set to "application/ vnd.3gpp.seal-user-profile-info+cbor";

c) shall include "ProfileDoc" object with "profileInformation" which:

   1) may contain "profileName" element indicating name of the profile;

   2) may contain "status" element indicating status of the profile;

   3) may contain "isDefault" element indicating that the current profile is the selected profile for the requesting user; and

   4) shall contain "profileConfig" elements; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [5].

6.2.5.4 SCM server CoAP procedure

Upon reception of an CoAP PUT request where the CoAP URI of the request identifies Individual User Profile resource as described in Annex C.2.1.2.3.3.2, the SCM-S:

a) shall determine the identity of the sender of the received CoAP PUT request as specified in clause 6.2.1.2, and:

   1) if the identity of the sender of the received CoAP PUT request is not authorized to update requested user profile document(s), shall respond with a CoAP 4.03 (Forbidden) response to the CoAP PUT request and skip rest of the steps;

b) shall support handling an CoAP PUT request from a SCM-C according to procedures specified in IETF RFC 7252 [12]; and

c) shall replace the user profile documents pointed at by the CoAP URI with the "ProfileDoc" received in the request.

6.3 Off-network procedures

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

7 Coding

7.1 VAL user profile document

7.1.1 General

7.1.2 Application unique ID

The AUID shall be set to the VAL service ID as specified in specific VAL service specification.

7.1.3 Data structure

The <seal-user-profile> element shall be the root element of the VAL user-profile configuration document.

The <seal-user-profile> element:

a) may include a <ProfileName> element;

b) shall include a <Status> element;

c) may include a <Pre-selected-indication> element;

d) shall include a <user-profile-index> element;

e) shall include a <profile-configuration> element;

   1) may include a <Common> element;

   2) may include a <OnNetwork> element; and

   3) may include a <OffNetwork> element; and

f) may include any other attribute for the purposes of extensibility.

7.1.4 XML Schema

The seal user profile configuration document shall be composed according to the following XML schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns="urn:3gpp:ns:seal:SealUserProfile:1.0"
  targetNamespace="urn:3gpp:ns:seal:SealUserProfile:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:sealup="urn:3gpp:ns:seal:SealUserProfile:1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:element name="seal-user-profile">
    <xs:complexType>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="ProfileName" type="sealup:NameType"/>
        <xs:element name="Status" type="xs:boolean"/>
        <xs:element name="isDefault" type="xs:boolean"/>
        <xs:element name="profile-configuration" type="sealup:ProfileConfigurationType"/>
        <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:choice>
      <xs:attribute name="user-profile-index" type="xs:unsignedByte" use="required"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="NameType">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attribute ref="xml:lang"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="ProfileConfigurationType">
    <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="Common" type="sealup:CommonType"/>
        <xs:element name="OnNetwork" type="sealup:OnNetworkType"/>
        <xs:element name="OffNetwork" type="sealup:OffNetworkType"/>
        <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>
  <xs:complexType name="CommonType" />
  <xs:complexType name="OnNetworkType" />
  <xs:complexType name="OffNetworkType" />
  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

7.1.5 Semantics

The <seal-user-profile> element is the root element of the XML document.

The <ProfileName> element of <seal-user-profile> element specifies the name of the SEAL user profile configuration document.

The <Status> element of <seal-user-profile> element is of type "Boolean" and indicates whether this particular SEAL user profile is enabled or disabled.

The <isDefault> element of <seal-user-profile> element is of type "Boolean" and indicates whether this particular SEAL user profile is default profile for VAL user or not.

The <user-profile-index> element of <seal-user-profile> element contains a positive number which provides profile id. This element is used only when multiple user-profile for a VAL user is supported.

The <profile-configuration> element of <seal-user-profile> element contains actual profile configuration. The VAL application which uses SEAL user-profile may provide its own profile configuration specific to VAL application.

The VAL service may further extend the <Common> element of the <profile-configuration> element of the <seal-user-profile> element to include VAL service specific common user profile configuration.

The VAL service may further extend the <OnNetwork> element of the <profile-configuration> element of the <seal-user-profile> element to include VAL service specific user profile configuration for on-network features.

The VAL service may further extend the <OffNetwork> element of the <profile-configuration> element of the <seal-user-profile> element to include VAL service specific user profile configuration for off-network features.

7.1.6 MIME type

The MIME type for VAL user profile configuration shall be set to "vnd.3gpp.seal-user-profile-info+xml".

7.1.7 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.seal-user-profile-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP or in HTTP. So the security considerations from IETF RFC 3261 apply while exchanging information in SIP and the security considerations from IETF RFC 2616 apply while exchanging information in HTTP.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.546 "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications Usage:

Applications supporting the SEAL configuration management procedures as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:

  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

  ii) Change controller: <MCC name>/<MCC email address>

7.2 VAL UE configuration document

7.2.1 General

7.2.2 Application unique ID

The AUID shall be set to the VAL service ID as specified in specific VAL service specification.

7.2.3 Data structure

The SEAL UE configuration document structure is specified in this clause.

The <seal-UE-configuration> document:

1) shall include a "domain" attribute;
2) may include a <VAL-UE-id> element;
3) may include a <VAL-service-id> element;
4) may include a <name> element;
5) may include a <common> element;
6) may include an <on-network> element; and
7) may include any other attribute for the purposes of extensibility.

The <VAL-UE-id> element:

1) may contain a list of <Instance-ID-URN> elements; and
2) may contain a list of <IMEI-range> elements.

The <IMEI-range> element:

1) shall contain a <TAC> element;
2) may contain a list of <SNR> elements; and
3) may contain <SNR-range> element.

The <SNR-range> element:

1) shall contain a <Low-SNR> element; and
2) shall contain a <High-SNR> element.

7.2.4 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns="urn:3gpp:ns:seal:sealUEConfig:1.0"
  targetNamespace="urn:3gpp:ns:seal:sealUEConfig:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:sealuec="urn:3gpp:ns:seal:sealUEConfig:1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">


  <xs:element name="seal-UE-configuration">
    <xs:complexType>
      <xs:sequence>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:element name="VAL-UE-id" type="sealuec:VALUEIDType"/>
          <xs:element name="VAL-service-id" type="xs:string"/>
          <xs:element name="name" type="sealuec:NameType"/>
        </xs:choice>
        <xs:element name="common" type="sealuec:CommonType"/>
        <xs:element name="on-network" type="sealuec:On-networkType"/>
        <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="domain" type="xs:anyURI" use="required"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="NameType">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attribute ref="xml:lang"/>
        <xs:attributeGroup ref="sealuec:IndexType"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="VALUEIDType">
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="Instance-ID-URN" type="xs:anyURI"/>
      <xs:element name="IMEI-range" type="sealuec:IMEI-rangeType"/>
      <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
    <xs:attributeGroup ref="sealuec:IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="IMEI-rangeType">
    <xs:sequence>
      <xs:element name="TAC" type="sealuec:tacType"/>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="SNR" type="sealuec:snrType"/>
        <xs:element name="SNR-range" type="sealuec:SNR-rangeType"/>
      </xs:choice>
      <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attributeGroup ref="sealuec:IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="SNR-rangeType">
    <xs:sequence>
      <xs:element name="Low-SNR" type="sealuec:snrType"/>
      <xs:element name="High-SNR" type="sealuec:snrType"/>
      <xs:element name="anyExt" type="sealuec:anyExtType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attributeGroup ref="sealuec:IndexType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="tac-baseType">
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="8"/>
      </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="tacType">
    <xs:simpleContent>
      <xs:extension base="sealuec:tac-baseType">
        <xs:attributeGroup ref="sealuec:IndexType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:simpleType name="snr-baseType">
    <xs:restriction base="xs:decimal">
      <xs:totalDigits value="6"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:complexType name="snrType">
    <xs:simpleContent>
      <xs:extension base="sealuec:snr-baseType">
        <xs:attributeGroup ref="sealuec:IndexType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="CommonType" />
  <xs:complexType name="On-networkType" />


  <xs:attributeGroup name="IndexType">
    <xs:attribute name="index" type="xs:token"/>
  </xs:attributeGroup>

  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

7.2.5 Semantics

The "domain" attribute of the <seal-UE-configuration> element contains the domain name of the VAL service.

The <name> element of the <seal-UE- configuration> element contains the user displayable name of the SEAL UE configuration document.

The creator of the SEAL UE configuration document may include an <VAL-UE-id> element in the version of the SEAL UE configuration document that is uploaded to the SCM-S. If an <VAL-UE-id> element is included then the SEAL UE configuration document applies only to the VAL UE(s) identified by the <VAL-UE-id> element. If no <VAL-UE-id> element is included then the SEAL UE configuration document applies to all the VAL UEs of the domain.

The <VAL-Service-id> element contains identify of the VAL service for which the configuration document is applicable.

If one or more optional <Instance-ID-URN> elements is included in the <VAL-UE-id> element then the SEAL UE configuration document applies to the VAL UE with an instance ID equal to the instance ID contained in the <Instance-ID-URN> element.

The <TAC> element of the <IMEI-range> element contains the Type Allocation Code of the VAL UE.

The optional <SNR> element of the <IMEI-range> element contains the individual serial number uniquely identifying VAL UE within the Type Allocation Code contained in the <TAC> element that the SEAL UE configuration document applies to.

If an optional <SNR-range> element is included within the <IMEI-range> element then the SEAL UE configuration document applies to all VAL UEs within the Type Allocation Code contained in the <TAC> element with the serial number equal or greater than the serial number contained in the <Low-SNR> element and less than or equal to the serial number contained in the <High-SNR> element.

If no <SNR> element nor <SNR-range> element is included within the <IMEI-range> element then the SEAL UE configuration document applies to all the VAL UE(s) with the Type Allocation Code contained within the <TAC> element of the <IMEI-range> element.

If no <VAL-UE-id> element is included then the SEAL UE configuration document applies to all VAL UEs of the VAL service identified in the "domain" attribute.

The VAL service may further extend the <Common> element of the <seal-UE-configuration> to include VAL service specific common UE configuration.

The VAL service may further extend the <on-network> element of the <seal-UE-configuration> to include VAL service specific UE configuration for on-network features.

7.2.6 MIME type

The MIME type for VAL user profile configuration shall be set to "vnd.3gpp.seal-ue-config-info+xml".

7.2.7 IANA registration template

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.seal-ue-config-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP or in HTTP. So the security considerations from IETF RFC 3261 apply while exchanging information in SIP and the security considerations from IETF RFC 2616 apply while exchanging information in HTTP.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.546 "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications Usage:

Applications supporting the SEAL configuration management procedures as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

  ii) Change controller: <MCC name>/<MCC email address>

Annex A (normative): Parameters for different operations

A.1 Creating configuration update event subscription

A.1.1 General

The information in this annex provides a normative description of the parameters which will be sent by SCM-C while creating configuration update event subscription and the parameters which will be sent by SCM-S as a response to request for creating subscription.

A.1.2 Client side parameters

The SCM-C shall convey the following parameters while sending request for creating configuration update event subscription.

Table A.1.2-1: Client side parameters for creating configuration update event subscription

Parameter	Description
Callback-URI	REQUIRED. Represents where to send HTTP notifications
Subscription Info	REQUIRED. Represents a space-separated list of the subscription type information as specified in table A.1.2-2.

Table A.1.2-2: Subscription information

Parameter	Description
Event	REQUIRED. Represents the type of notification which client requires. This specification defines following type of notifications: - 0x01: SUBSCRIBE_USER_PROFILE_MODIFICATION - 0x02: SUBSCRIBE_UE_CONFIG_MODIFICATION
expiry time	REQUIRED. Represents the time in seconds up to which the subscription is desired to be kept active and the time after which the subscribed event shall stop generating notifications.

A.1.3 Server side parameters

The SCM-S shall convey the following parameters while sending response to the creating configuration update event subscription request.

Table A.1.3-1: Server side parameters for response to creating configuration update event subscription

Parameter	Description
Identity	REQUIRED. A unique string representing subscription identity.

A.2 Retrieve VAL UE configuration data

A.2.1 Client side parameters

The SGM-C shall convey the following parameters, if available, while sending request to retrieve a VAL UE configuration data.

Table A.1.2-1: Client side parameters to retrieve VAL UE configuration data

Parameter	Description
VAL UE Information	OPTIONAL. Represents additional UE related information required to identify the configuration data (e.g. device type, device vendor, etc).

Annex B (normative): Parameters for notifications

B.1 General

The information in this annex provides a normative description of the parameters which will be sent by SCM-S while sending different types of notification

B.2 Configuration update notification

The SCM-S shall convey the following parameters while sending configuration notification to SCM-C.

Table B.2-1: Parameters for configuration update notification

Parameter	Description
Identity	REQUIRED. A unique string representing notification channel identity.
Event	REQUIRED. Shall be set to one of the event as specified in table A.1.2-2 based on which configuration document is updated.

Annex C (normative): CoAP resource representation and encoding

C.1 General

The information in this annex provides a normative description of CoAP resource representation and encoding.

C.1.1 Resource URI structure

All API URIs of SEAL-UU APIs shall be specified as follows:

{apiRoot}/<apiName>/<apiVersion>

"apiRoot" is configured by means outside the scope of the present document. It includes one of the schemes ("coaps", "coaps+tcp", "coaps+ws"), host and optional port, and an optional prefix string. "apiName" and "apiVersion" shall be set dependent on the API, as defined in the corresponding clauses below.

All resource URIs specified for SEAL-UU APIs shall be defined relative to the above root API URI.

URIs which differ only in the scheme shall point to the same resource.

NOTE: The "apiVersion" will only be increased if the new API version contains backward incompatible changes.

The root structure may be followed by "apiSpecificSuffixes" that are dependent on the API and are defined separately for each API as resource URI where they apply:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificSuffixes>

C.1.2 Use of cache

It is recommended for the SEAL clients and servers to support and use the caching mechanism specified in IETF RFC 7252 [12]. This implies support and use of the Max-Age and ETag options.

C.1.3 Error handling

Table C.1.3-1 lists response payload types that are applicable to all APIs and as responses for all requests in the present specification unless otherwise specified. The CoAP client shall mandatorily support the processing of the status code for all the applicable methods, when received in a CoAP response message.

Table C.1.3-1: Response payloads supported for responses to all requests.

	Data type	Cardinality	Response Codes (NOTE)	Remarks	Applied Methods
Response body	ProblemDetails	1	4.00 Bad Request	Incorrect parameters were passed in the request.	GET, POST PUT, PATCH, DELETE
	ProblemDetails	1	4.01 Unauthorized	The client is not authorized.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	4.02 Bad Option	The request could not be understood by the server due to one or more unrecognized or malformed options.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	4.03 Forbidden	This represents the case when the server is able to understand the request but unable to fulfil the request due to errors (e.g. the requested parameters are out of range). More information may be provided in the "invalidParams" attribute of the "ProblemDetails" structure.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	4.04 Not Found	The resource URI was incorrect.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	4.06 Not Acceptable	The content format provided in the "Accept" option is not acceptable by the server.	GET
	ProblemDetails	1	4.13 Request Entity Too Large	If the received CoAP request contains entity larger than the server is able to process, the server shall reject the CoAP request with this status code. The server should include Size1 option in the response with the maximum size of the request entity it can handle.	POST, PUT, PATCH
	ProblemDetails	1	4.15 Unsupported Content-Format	The code indicates that the resource is in a format which is not supported by the server for the method.	POST, PUT, PATCH
	ProblemDetails	1	4.29 Too Many Requests	The code indicates that due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation. The CoAP option "Max-Age" may be added in the response to indicate how long the client has to wait before making a new request.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	5.00 Internal Server Error	The server encountered an unexpected condition that prevented it from fulfilling the request.	GET, POST, PUT, PATCH, DELETE
	ProblemDetails	1	5.03 Service Unavailable	The server is unable to handle the request.	GET, POST, PUT, PATCH, DELETE

NOTE: In addition to the above response codes, the CoAP server may also send other valid CoAP response codes, if applicable. The list of all valid CoAP response codes can be found in CoAP Response Code Registry at IANA [19].

Editor's Note: Handling of "ProblemDetails" indicated in Table C.1.3-1 based on the IETF draft [20] is FFS.

Editor's Note: Handling of the PATCH method indicated in Table C.1.3-1 is FFS.

Specific errors are contained in the related API definition for each API.

C.1.4 Data types applicable to multiple resource representations

C.1.4.1 General

This clause defines structured data types, simple data types, and enumerations that are applicable to several APIs defined for CoAP resource representations in the present specification and other SEAL specifications and can be referenced from data structures defined in the subsequent clauses and from CoAP resource representations in other SEAL specifications.

NOTE: As a convention, data type names in the present specification follows UpperCamel and parameters follows lowerCamel as specified in clause 5.1.1 of 3GPP TS 29.501 [23].

C.1.4.2 Referenced structured data types

Table C.1.4.2-1 lists structured data types referenced by multiple CoAP resource representations and defined in this specification or in other specifications.

Table C.1.4.2-1: Referenced Structured Data Types

Data type	Reference	Description
ValTargetUe	Clause C.2.1.4.2.4	Information identifying a VAL user ID or VAL UE ID.
ScheduledCommunicationTime	Clause C.1.4.4.1	Defines time schedule for communication.

C.1.4.3 Referenced simple data types and enumerations

The simple datatypes based on the CBOR types are defined in table C.1.4.3-1 and the simple data types defined in table 5.2.1.3.2-2 apply to multiple SEAL-UU APIs.

Table C.1.4.3-1: CBOR-based data types

Type name	Description
bytes	Is a "byte string" as defined in IETF RFC 8949 [17].
boolean	Is a type which has 2 values "false" and "true" with the values as defined in IETF RFC 8949 [17].
integer	As defined in IETF RFC 8949 [17].
number	Is any number as defined in IETF RFC 8949 [17]. Precision format (half-precision, single-precision, and double-precision) can be indicated.
string	Is a "text string" as defined in IETF RFC 8949 [17].

Table C.1.4.3-2: Simple data types applicable to multiple CoAP resource representations

Type name	Description
ExternalGroupId	String containing a local identifier followed by "@" and a domain identifier. Both the local identifier and the domain identifier shall be encoded as strings that do not contain any "@" characters. See Clauses 4.6.2 and 4.6.3 of 3GPP TS 23.682[24] for more information.
DateTime	Is a string in the standard format described by the "date-time" production in IETF RFC3339 [25].
DayOfWeek	Integer between and including 1 and 7 denoting a weekday. 1 shall indicate Monday, and the subsequent weekdays shall be indicated with the next higher numbers. 7 shall indicate Sunday.
TimeOfDay	String with format partial-time or full-time as defined in clause 5.6 of IETF RFC 3339 [25]. Examples, 20:15:00, 20:15:00-08:00 (for 8 hours behind UTC).
Uinteger	Unsigned integer, i.e. only value 0 and values above 0 are permissible.
Uri	String providing an URI formatted according to IETF RFC 3986 [22].

Table C.1.4.3-3 lists simple data types and enumerations referenced by multiple CoAP resource representations defined in this specification or in other specifications.

Table C.1.4.3-3: Enumerations applicable to multiple CoAP resource representations

Type name	Reference	Description
ConfigType	C.2.1.4.3.1	Represents the type of configuration.

C.1.4.4 Common structured data types

C.1.4.4.1 Type: ScheduledCommunicationTime

Table C.1.4.4.1-1: Definition of type ScheduledCommunicationTime

Attribute name	Data type	P	Cardinality	Description	Applicability
daysOfWeek	array(DayOfWeek)	O	0..6	Identifies the day(s) of the week. If absent, it indicates every day of the week.	
timeOfDayStart	TimeOfDay	O	0..1	Identifies the start time of the day.	
timeOfDayEnd	TimeOfDay	O	0..1	Identifies the end time of the day.	

C.1.4.5 Common enumerations

None.

C.2 Resource representation and APIs for VAL user profile

C.2.1 SU_UserProfile API

C.2.1.1 API URI

The CoAP URIs used in CoAP requests from SCM-C towards the SCM-S shall have the Resource URI structure as defined in clause C.1.1 with the following clarifications:

- the <apiName> shall be "su-up";
- the <apiVersion> shall be "v1"; and

- the <apiSpecificSuffixes> shall be set as described in clause C.2.1.2.

C.2.1.2 Resources

C.2.1.2.1 Overview

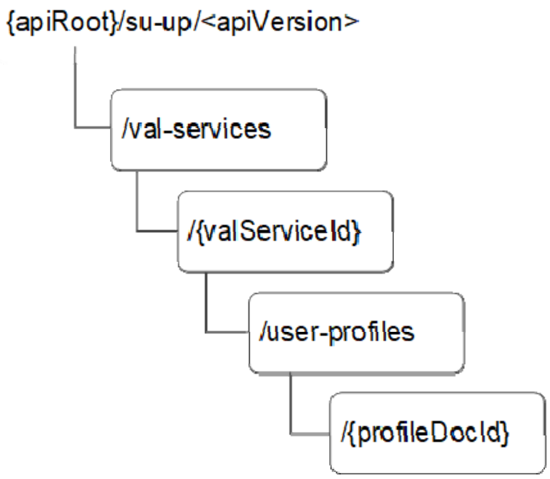

Figure C.2.1.2.1-1: Resource URI structure of the SU_UserProfile API

Table C.2.1.2.1-1 provides an overview of the resources and applicable CoAP methods.

Table C.2.1.2.1-1: Resources and methods overview

Resource name	Resource URI	CoAP method	Description
User Profiles	/val-services/{valServiceId}/user-profiles	GET	Retrieve VAL user or VAL UE's user profiles for a given VAL service, according to query criteria.
		POST	Create user profile.
Individual User Profile	/val-services/{valServiceId}/user-profiles/{profileDocId}	GET	Retrieve an individual user profile.
		PUT	Update an individual user profile.
		DELETE	Delete an individual user profile.

Editor's note: Whether any changes required in the API along with its data model based on limitations of constrained devices is FFS.

C.2.1.2.2 Resource: User Profiles

C.2.1.2.2.1 Description

The User Profiles resource allows a SCM-C to retrieve all the user profiles of a VAL user or a VAL UE for a specific VAL service that are available at a given SCM-S, or allows to create a new user profile.

C.2.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/su-up/<apiVersion>/val-services/{valServiceId}/user-profiles**

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

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

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

C.2.1.2.2.3 Resource Standard Methods

C.2.1.2.2.3.1 GET

This operation retrieves VAL **u**ser or VAL UE profile information satisfying the filter criteria.

This method shall support the URI query parameters specified in table C.2.1.2.2.3.1-1.

Table C.2.1.2.2.3.1-1: URI query parameters supported by the GET Request on this resource

Name	Data type	P	Cardinality	Description
val-tgt-ue	ValTargetUe	M	1	Identifies a VAL target UE.

This method shall support the response data structures and response codes specified in table C.2.1.2.2.3.1-2.

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

Data type	P	Cardinality	Response codes	Description
array(ProfileDoc)	M	0..N	2.05 Content	List of VAL user / VAL UE profile documents. This response shall include user profile information matching the query parameters provided in the request.
NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 shall also apply.				

C.2.1.2.2.3.2 POST

This operation creates a VAL user or VAL UE profile information at the SCM-S for a given VAL service.

This method shall support the request data structures specified in table C.2.1.2.2.3.2-1, the response data structures and response codes specified in table C.2.1.2.2.3.2-2, and the response options specified in table C.2.1.2.2.3.2-3.

Table C.2.1.2.2.3.2-1: Data structures supported by the POST Request payload on this resource

Data type	P	Cardinality	Description
ProfileDoc	M	1	The user profile document to be created for a VAL user or VAL UE.

Table C.2.1.2.2.3.2-2: Data structures supported by the POST Response payload on this resource

Data type	P	Cardinality	Response codes	Description
ProfileDoc	O	0..1	2.01 Created	The user profile was created successfully. The "profileDocId" of the created resource shall be returned in the "Location-Path" option.
NOTE: The mandatory CoAP error status codes for the POST method listed in table C.1.3-1 shall also apply.				

Table C.2.1.2.2.3.2-3: Options supported by the 2.01 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location-Path	string	M	1	Contains the location path of the newly created resource relative to the request URI. It contains the profileDocId segment of the complete resource URI according to the structure: {apiRoot}/su-up/<apiVersion>/val-services/{valServiceId}/user-profiles/{profileDocId}

C.2.1.2.3 Resource: Individual User Profile

C.2.1.2.3.1 Description

The Individual User Profile resource represents an individual user profile that is created at the SCM-S for a given VAL service. This resource is observable.

C.2.1.2.3.2 Resource Definition

Resource URI: **{apiRoot}/su-up/<apiVersion>/val-services/{valServiceId}/user-profiles/{profileDocId}**

This resource shall support the resource URI variables defined in the table C.2.1.2.3.2-1.

Table C.2.1.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause C.1.1
apiVersion	string	See clause C.2.1.1
valServiceId	string	Identifier of a VAL service.
profileDocId	string	Represents an individual user profile resource.

C.2.1.2.3.3 Resource Standard Methods

C.2.1.2.3.3.1 GET

This operation retrieves the user profile document.

This method shall support the request options specified in table C.2.1.2.3.3.1-1, the response data structures and response codes specified in table C.2.1.2.3.3.1-2, and the response options specified in table C.2.1.2.3.3.1-3.

Table C.2.1.2.3.3.1-1: Options supported by the GET Request on this resource

Name	Data type	P	Cardinality	Description
Observe	Uinteger	O	0..1	When set to 0 (Register) it extends the GET request to subscribe to the changes of this resource. When set to 1 (Deregister) it cancels the subscription.
NOTE: Other request options also apply in accordance with normal CoAP procedures.				

Table C.2.1.2.3.3.1-2: Data structures supported by the GET Response payload on this resource

Data type	P	Cardinality	Response codes	Description
ProfileDoc	M	1	2.05 Content	The User profile information based on the request from the SCM-C.
NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 shall also apply.				

Table C.2.1.2.3.3.1-3: Options supported by the 2.05 Response Code on this resource

Name	Data type	P	Cardinality	Description
Observe	Uinteger	O	0..1	Sequence number of the notification.
NOTE: Other response options also apply in accordance with normal CoAP procedures.				

C.2.1.2.3.3.2 PUT

This operation updates the user profile document.

This method shall support the request data structures specified in table C.2.1.2.3.3.2-1 and the response data structures and response codes specified in table C.2.1.2.3.3.2-2.

Table C.2.1.2.3.3.2-1: Data structures supported by the PUT Request payload on this resource

Data type	P	Cardinality	Description
ProfileDoc	M	1	Updated details of the user profile document.

Table C.2.1.2.3.3.2-2: Data structures supported by the PUT Response payload on this resource

Data type	P	Cardinality	Response codes	Description
ProfileDoc	O	0..1	2.04 Changed	The user profile document updated successfully and the updated user profile document may be returned in the response.
NOTE: The mandatory CoAP error status codes for the PUT method listed in table C.1.3-1 shall also apply.				

C.2.1.2.3.3.3 DELETE

This operation deletes the user profile document.

This method shall support the response data structures and response codes specified in table C.2.1.2.3.3.3-1.

Table C.2.1.2.3.3.3-1: Data structures supported by the DELETE Response payload on this resource

Data type	P	Cardinality	Response codes	Description
n/a			2.02 Deleted	The individual User profile document matching the profileDocId is deleted.
NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 shall also apply.				

C.2.1.3 Data Model

C.2.1.3.1 General

Table C.2.1.3.1-1 specifies the data types defined specifically for the SU_UserProfile API service.

Table C.2.1.3.1-1: SU_UserProfile API specific Data Types

Data type	Section defined	Description	Applicability
ProfileDoc	C.2.1.3.2.1	Profile information associated with VAL user ID or VAL UE ID.	
ProfileInfo	C.2.1.3.2.2	Profile information including profile configurations.	
ProfileConfig	C.2.1.3.2.3	Profile configuration including configuration data.	
ConfigType	C.2.1.3.3.1	Specifies type of features for which the configuration data is applicable.	
ValTargetUe	C.2.1.3.2.4	Information identifying a VAL user ID or VAL UE ID.	

C.2.1.3.2 Structured data types

C.2.1.3.2.1 Type: ProfileDoc

Table C.2.1.3.2.1-1: Definition of type ProfileDoc

Attribute name	Data type	P	Cardinality	Description	Applicability
profileDocId	string	O	0..1	Contains the profileDocId of the complete resource URI of this user profile document according to the structure: {apiRoot}/su-up/<apiVersion>/val-services/{valServiceId}/user-profiles/{profileDocId} This attribute shall be provided by the SCM-S in CoAP responses.	
profileInformation	ProfileInfo	M	1	Profile information associated with a VAL user or a VAL UE as specified in valTgtUe.	
valTgtUe	ValTargetUe	M	1	Unique identifier of a VAL user or a VAL UE.	

C.2.1.3.2.2 Type: ProfileInfo

Table C2.1.4.2.2-1: Definition of type ProfileInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
profileName	string	O	0..1	Name of the user profile.	
status	boolean	M	1	Indicates whether the user profile is enabled or disabled.	
array(ProfileConfig)	ProfileConfig	O	1..N	List of profile configurations.	
isDefault	boolean	O	0..1	Indicates whether the user profile is the default profile for VAL user or not.	

C.2.1.3.2.3 Type: ProfileConfig

Table C.2.1.3.2.3-1: Definition of type ProfileConfig

Attribute name	Data type	P	Cardinality	Description	Applicability
configType	ConfigType	M	1	Indicates the type of the profile configuration.	
configData	string	M	1	Actual user profile configuration data.	

C.2.1.3.2.4 Type: ValTargetUe

Table C.2.1.3.2.4-1: Definition of type ValTargetUe

Attribute name	Data type	P	Cardinality	Description	Applicability
valUserId	string	O	0..1	Unique identifier of a VAL user.	
valUeId	string	O	0..1	Unique identifier of a VAL UE.	
NOTE: Either "valUserId" or "valUeId" shall be present.					

C.2.1.3.3 Simple data types and enumerations

C.2.1.3.3.1 Enumeration: ConfigType

Table C.2.1.3.3.1-1: Enumeration ConfigType

Enumeration value	Description	Applicability
COMMON	Indicates VAL service specific configuration for common features.	
ON_NETWORK	Indicates VAL service specific configuration for on-network features.	
OFF_NETWORK	Indicates VAL service specific configuration for off-network features.	

C.2.1.4 Error Handling

General error responses are defined in clause C.1.3.

C.2.1.5 CDDL Specification

C.2.1.5.1 Introduction

The data model described in clause C.2.1.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [17].

Clause C.2.1.5.2 uses the Concise Data Definition Language described in IETF RFC 8610 [18] and provides corresponding representation of the SU_UserProfile API data model.

C.2.1.5.2 CDDL document

```
;;; ProfileDoc
;;+ Represents user profile information associated with a VAL user ID or a VAL UE ID.

ProfileDoc = {
 ? profileDocId: text
 profileInformation: ProfileInfo
 valTgtUe: ValTargetUe
}

;;; ValTargetUe
;;+ Represents information identifying a VAL user ID or a VAL UE ID.

ValTargetUe = {
 (
 valUserId: text                 ; Unique identifier of a VAL user.
 //
 valUeId: text                   ; Unique identifier of a VAL UE.
 )
}
```

```
;;; ProfileInfo
;;+ User profile information.

ProfileInfo = {
 ? profileName: text             ; Name of the profile
 status: bool                    ; Indicates whether the user profile is enabled or disabled.
? profileConfigs: [+ ProfileConfig]
 ? isDefault: bool               ; Indicates whether the user profile is the default profile for VAL
user or not.
}

;;; ProfileConfig
;;+ Profile configuration.

ProfileConfig = {
 configType: ConfigType
 configData: text                ; Actual user profile configuration data.
}

;;; ConfigType
;;+ Indicates the type of the configuration.

ConfigType = "COMMON" / "ON_NETWORK" / "OFF_NETWORK" / text
```

C.2.1.6 Media Type

The media type for a user profile document shall be "application/vnd.3gpp.seal-user-profile-info+cbor".

Editor's Note: It is possible to specify other payload format for CoAP than CBOR, and the details about other payload format is FFS.

C.2.1.8 Media Type registration for application/vnd.3gpp.seal-user-profile-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-user-profile-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [17]. See 3GPP TS 24.546 clause C.2.1.3 for details.

Security considerations: See Section 10 of IETF RFC 8949 [17] and Section 11 of IETF RFC 7252 [12].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.546 "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL configuration management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [17]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

Editor's Note: The registration for application/vnd.3gpp.seal-user-profile-info+cbor is TBD.

C.3 Resource representation and APIs for UE configuration

C.3.1 SU_UeConfig API

C.3.1.1 API URI

The CoAP URIs used in CoAP requests from SCM-C towards the SCM-S shall have the Resource URI structure as defined in clause C.1.1 with the following clarifications:

- the <apiName> shall be "su-uc";
- the <apiVersion> shall be "v1"; and
- the <apiSpecificSuffixes> shall be set as described in clause C.3.1.2.

C.3.1.2 Resources

C.3.1.2.1 Overview

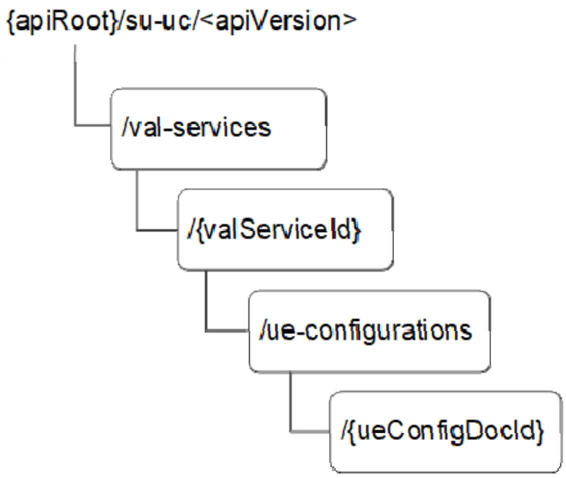

Figure C.3.1.2.1-1: Resource URI structure of the SU_UeConfig API

Table C.3.1.2.1-1 provides an overview of the resources and applicable CoAP methods.

Table C.3.1.2.1-1: Resources and methods overview

Resource name	Resource URI	CoAP method	Description
UE Configurations	/val-services/{valServiceId}/ue-configurations	GET	Retrieve UE configurations for a given VAL service, according to query criteria.
		POST	Create UE configuration.
Individual UE Configuration	/val-services/{valServiceId}/ue-configurations/{ueConfigDocId}	GET	Retrieve an individual UE configuration.
		PUT	Update an individual UE configuration.
		DELETE	Delete an individual UE configuration.

Editor's note: Whether any changes required in the API along with its data model based on limitations of constrained devices is FFS.

C.3.1.2.2 Resource: UE Configurations

C.3.1.2.2.1 Description

The UE Configurations resource allows a SCM-C to retrieve all the UE configurations of a VAL service domain (e.g. based on device type, device vendor, device number, etc) for a specific VAL service that are available at a given SCM-S.

C.3.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/su-uc/<apiVersion>/val-services/{valServiceId}/ue-configurations**

This resource shall support the resource URI variables defined in the table C.3.1.2.2.2-1.

Table C.3.1.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause C.1.1
apiVersion	string	See clause C3.1.1
valServiceId	string	Identifier of a VAL service.

C.3.1.2.2.3 Resource Standard Methods

C.3.1.2.2.3.1 GET

This operation retrieves UE configurations satisfying the query criteria.

This method shall support the URI query parameters specified in table C.3.1.2.2.3.1-1.

Table C.3.1.2.2.3.1-1: URI query parameters supported by the GET Request on this resource

Name	Data type	P	Cardinality	Description
ue-vendor	string	O	0..1	Identity of the UE vendor.
ue-type	TypeAllocationCode	O	0..1	Type of the UE.
ue-snr	SerialNumber	O	0..1	Serial number of the UE.
ue-uri	Uri	O	0..1	URI of the UE.

This method shall support the response data structures and response codes specified in table C.3.1.2.2.3.1-2.

Table C.3.1.2.2.3.1-2: Data structures supported by the GET Response payload on this resource

Data type	P	Cardinality	Response codes	Description
array(UeConfigDoc)	M	0..N	2.05 Content	List of UE configuration documents matching any of the query parameters provided in the request. If no query parameters are given, all the UE configuration documents are returned.
NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 shall also apply.				

C.3.1.2.2.3.2 POST

This operation creates a UE configuration at the SCM-S for a given VAL service.

This method shall support the request data structures specified in table C.3.1.2.2.3.2-1, the response data structures and response codes specified in table C.3.1.2.2.3.2-2, and the response options specified in table C.3.1.2.2.3.2-3.

Table C.3.1.2.2.3.2-1: Data structures supported by the POST Request payload on this resource

Data type	P	Cardinality	Description
UeConfigDoc	M	1	The UE configuration to be created.

Table C.3.1.2.2.3.2-2: Data structures supported by the POST Response payload on this resource

Data type	P	Cardinality	Response codes	Description
UeConfigDoc	O	0..1	2.01 Created	The UE configuration was created successfully. The "ueConfigDocId" of the created resource shall be returned in the "Location-Path" option.
NOTE: The mandatory CoAP error status codes for the POST method listed in table C.1.3-1 shall also apply.				

Table C.3.1.2.2.3.2-3: Options supported by the 2.01 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location-Path	string	M	1	Contains the location path of the newly created resource relative to the request URI. It contains the ueConfigDocId segment of the complete resource URI according to the structure: {apiRoot}/su-uc/<apiVersion>/val-services/{valServiceId}/ue-configurations/{ueConfigDocId}

C.3.1.2.3 Resource: Individual UE Configuration

C.3.1.2.3.1 Description

The Individual UE Configuration resource represents an individual UE configuration stored at the SCM-S for a given VAL service. This resource is observable.

C.3.1.2.3.2 Resource Definition

Resource URI: **{apiRoot}/su-uc/<apiVersion>/val-services/{valServiceId}/ue-configurations/{ueConfigDocId}**

This resource shall support the resource URI variables defined in the table C.3.1.2.3.2-1.

Table C.3.1.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause C.1.1
apiVersion	string	See clause C.2.1.1
valServiceId	string	Identifier of a VAL service.
ueConfigDocId	string	Represents an individual UE configuration resource.

C.3.1.2.3.3 Resource Standard Methods

C.3.1.2.3.3.1 GET

This operation retrieves the UE configuration document.

This method shall support the request options specified in table C.3.1.2.3.3.1-1, the response data structures and response codes specified in table C.3.1.2.3.3.1-2, and the response options specified in table C.3.1.2.3.3.1-3.

Table C.3.1.2.3.3.1-1: Options supported by the GET Request on this resource

Name	Data type	P	Cardinality	Description
Observe	Uinteger	O	0..1	When set to 0 (Register) it extends the GET request to subscribe to the changes of this resource. When set to 1 (Deregister) it cancels the subscription.
NOTE: Other request options also apply in accordance with normal CoAP procedures.				

Table C.3.1.2.3.3.1-2: Data structures supported by the GET Response payload on this resource

Data type	P	Cardinality	Response codes	Description
UeConfigDoc	M	1	2.05 Content	The UE configuration based on the request from the SCM-C.
NOTE: The mandatory CoAP error status codes for the GET Request listed in table C.1.3-1 shall also apply.				

Table C.3.1.2.3.3.1-3: Options supported by the 2.05 Response Code on this resource

Name	Data type	P	Cardinality	Description
Observe	Uinteger	O	0..1	Sequence number of the notification.
NOTE: Other response options also apply in accordance with normal CoAP procedures.				

C.3.1.2.3.3.2 PUT

This operation updates the UE configuration document.

This method shall support the request data structures specified in table C.3.1.2.3.3.2-1 and the response data structures and response codes specified in table C.3.1.2.3.3.2-2.

Table C.3.1.2.3.3.2-1: Data structures supported by the PUT Request payload on this resource

Data type	P	Cardinality	Description
UeConfigDoc	M	1	Updated details of the UE configuration document.

Table C.3.1.2.3.3.2-2: Data structures supported by the PUT Response payload on this resource

Data type	P	Cardinality	Response codes	Description
UeConfigDoc	O	1	2.04 Changed	The UE configuration document updated successfully and the updated UE configuration document may be returned in the response.
NOTE: The mandatory CoAP error status codes for the PUT method listed in table C.1.3-1 shall also apply.				

C.3.1.2.3.3.3 DELETE

This operation deletes the UE configuration document.

This method shall support the response data structures and response codes specified in table C.3.1.2.3.3.3-1.

Table C.3.1.2.3.3.3-1: Data structures supported by the DELETE Response payload on this resource

Data type	P	Cardinality	Response codes	Description
n/a			2.02 Deleted	The individual UE configuration document matching the ueConfigDocId is deleted.
NOTE: The mandatory CoAP error status codes for the DELETE method listed in table C.1.3-1 shall also apply.				

C.3.1.3 Data Model

C.3.1.3.1 General

Table C.3.1.3.1-1 specifies the data types defined specifically for the SU_UeConfig resource representation.

Table C.3.1.3.1-1: SU_UeConfig API specific data types

Data type	Section defined	Description	Applicability
UeConfigDoc	C.3.1.4.2.1	UE configuration document.	
UeConfig	C.3.1.4.2.2	UE configuration including configuration data.	
ValUeIds	C.3.1.4.2.3	VAL UE identifiers.	
ImeiRange	C.3.1.3.2.4	Range of IMEIs.	
SnrRange	C.3.1.3.2.5	Range of UE serial numbers.	
SerialNumber	C.3.1.3.3.1	Serial number of a UE.	
TypeAllocationCode	C.3.1.3.3.1	Type allocation code.	

Table C.3.1.3.1-2 specifies data types re-used by the SS_Events API service:

Table C.3.1.3.1-2: Reused data types

Data type	Reference	Comments	Applicability
ConfigType	C.2.1.3.3.1	Configuration type.	
Uri	C.1.4.3	Unified resource identifier.	

C.3.1.3.2 Structured data types

C.3.1.3.2.1 Type: UeConfigDoc

Table C.3.1.3.2.1-1: Definition of type UeConfigDoc

Attribute name	Data type	P	Cardinality	Description	Applicability
ueConfigDocId	string	O	0..1	Contains the ueConfigDocId of the complete resource URI of this UE configuration document according to the structure: {apiRoot}/su-uc/<apiVersion>/val-services/{valServiceId}/ue-configurations/{ueConfigDocId} This attribute shall be provided by the SCM-S in CoAP responses.	
configName	string	O		Displayable name of the UE configuration document.	
valServiceDomain	string	M	1	Domain name of the VAL service for which the configuration document is applicable.	
valServiceId	string	O	0..1	VAL service identity for which the configuration document is applicable.	
valUeIds	ValUeIds	O	0..1	Defines a set of VAL UE IDs for which the configuration document is applicable.	
ueConfigs	array(UeConfig)	O	1..N	List of UE configurations of different configuration types, i.e. there shall not be 2 configuration with the same value of configType.	

C.3.1.3.2.2 Type: UeConfig

Table C.3.1.3.2.2-1: Definition of type UeConfig

Attribute name	Data type	P	Cardinality	Description	Applicability
configType	ConfigType (NOTE)	M	1	Indicates the type of the UE configuration.	
configData	string	M	1	Actual UE configuration data.	
NOTE: Only the values COMMON and ON_NETWORK are applicable in the present specification.					

C.3.1.3.2.3 Type: ValUeIds

Table C.3.1.3.2.3-1: Definition of type ValUeIds

Attribute name	Data type	P	Cardinality	Description	Applicability
uris	array(Uri)	O	1..N	List of VAL UE identities, each identity defined by a URI.	
imeiRanges	array(ImeiRange)	O	1..N	List of IMEI ranges.	

C.3.1.3.2.4 Type: ImeiRange

Table C.3.1.3.2.4-1: Definition of type ImeiRange

Attribute name	Data type	P	Cardinality	Description	Applicability
tac	TypeAllocationCode	M	1	Type allocation code of the UEs.	
snrs	array(SerialNumber)	O	1..N	List of UE serial numbers.	
snrRange	SnrRange	O	0..1	Range of UE serial numbers.	

C.3.1.3.2.5 Type: SnrRange

Table C.3.1.3.2.5-1: Definition of type SnrRange

Attribute name	Data type	P	Cardinality	Description	Applicability
low	SerialNumber	M	1	First UE serial number identifying the start of a UE serial number range.	
high	SerialNumber	M	1	Last UE serial number identifying the end of a UE serial number range.	

C.3.1.3.3 Simple data types and enumerations

C.3.1.3.3.1 Simple data types

Table C.3.1.3.3.1-1: Simple data types

Type Name	Type Definition	Description
TypeAllocationCode	string	Type Allocation Code (TAC) of the UE, comprising the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEISV codes. See clause 6.2 of 3GPP TS 23.003 [26]. Pattern: '^[0-9]{8}$'
SerialNumber	string	Serial number of the UE, comprising the six-digit portion of the 15-digit IMEI and 16-digit IMEISV codes. See clause 6.2 of 3GPP TS 23.003 [26]. Leading 0s may be excluded. Pattern: '^[0-9]{1,6}$'

C.3.1.4 Error Handling

General error responses are defined in clause C.1.3.

C.3.1.5 CDDL Specification

C.3.1.5.1 Introduction

The data model described in clause C.3.1.3 shall be binary encoded in the CBOR format as described in IETF RFC 8949 [17].

Clause C.3.1.5.2 uses the Concise Data Definition Language described in IETF RFC 8610 [18] and provides corresponding representation of the SU_UeConfig API data model.

C.3.1.5.2 CDDL document

```
;;; UeConfigDoc
;;+ Represents UE configuration information associated with a VAL service.

UeConfigDoc = {
 ? UeConfigDocId: text
 ? configName: text             ; Name of the config
 valServiceDomain: text
 ? valServiceId: text
 ? valUeIds: ValUeIds
 ? ueConfigs: [+ UeConfig]
}

;;; UeConfig
;;+ UE configuration.

UeConfig = {
 configType: ConfigType
 configData: text                ; Actual UE configuration  data.
}

;;; ConfigType
;;+ Indicates the type of the UE configuration.

ConfigType = "COMMON" / "ON_NETWORK" / text

;;; ValUeIds
;;+ VAL UE identities for which the UE configuration is applicable.

ValUeIds = {
 ? uris: [+ Uri]
 ? imeiRanges: [+ ImeiRange]
}

;;; ImeiRange
;;+ Defines a range of IMEIs.

ImeiRange = {
 tac: TypeAllocationCode
 ? snrs: [+ SerialNumber]
 ? snrRange: SnrRange
}

;;; SnrRange
;;+ Defines a range of SerialNumbers.

SnrRange = {
 low: SerialNumber
 high: SerialNumber
}

;;; TypeAllocationCode
;;+ Type Allocation Code.

TypeAllocationCode = text .regexp "[0-9]{8}"

;;; SerialNumber
;;+ Serial Number.

SerialNumber = text .regexp "[0-9]{1,6}" ;

;;; Uri
;;+ URI

Uri = text          ; formatted according to RFC 3986
```

C.3.1.6 Media Type

The media type for a user profile document shall be "application/vnd.3gpp.seal-ue-config-info+cbor".

Editor's Note: It is possible to specify other payload format for CoAP than CBOR, and the details about other payload format is FFS.

C.3.1.7 Media Type registration for application/vnd.3gpp.seal-ue-config-info+cbor

Type name: application

Subtype name: vnd.3gpp.seal-ue-config-info+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Must be encoded as using IETF RFC 8949 [17]. See 3GPP TS 24.546 clause C.3.1.3 for details.

Security considerations: See Section 10 of IETF RFC 8949 [17] and Section 11 of IETF RFC 7252 [12].

Interoperability considerations: Applications must ignore any key-value pairs that they do not understand. This allows backwards-compatible extensions to this specification.

Published specification: 3GPP TS 24.546 "Configuration management - Service Enabler Architecture Layer for Verticals (SEAL); Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Applications that use this media type: Applications supporting the SEAL configuration management procedures as described in the published specification.

Fragment identifier considerations: Fragment identification is the same as specified for "application/cbor" media type in IETF RFC 8949 [17]. Note that currently that RFC does not define fragmentation identification syntax for "application/cbor".

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): none

Macintosh file type code(s): none

Person & email address to contact for further information: <MCC name>, <MCC email address>

Intended usage: COMMON

Restrictions on usage: None

Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

Change controller: <MCC name>/<MCC email address>

Editor's Note: The registration for application/vnd.3gpp.seal-ue-config-info+cbor is TBD.

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-09	CT1#120	C1-196120				Draft skeleton provided by the rapporteur.	0.0.0
2019-10	CT1#120					Implementing the following p-CR agreed by CT1: C1-196607, C1-196609, C1-196853, C1-196854	0.1.0
2019-11	CT1#121					Implementing the following p-CR agreed by CT1: C1-198620, C1-198815, C1-198816	0.2.0
2019-12	CT-86	CP-193153				Presentation for information at TSG CT	1.0.0
2020-02	CT1#122-e					Implementing the following p-CR agreed by CT1: C1-200645, C1-200646, C1-200873, C1-200872, C1-200649, C1-201005, C1-200823	1.1.0
2020-03	CT-87e	CP-200170				Presentation for approval at TSG CT	2.0.0
2020-03	CT-87e					Version 16.0.0 created after approval	16.0.0
2020-06	CT-88e	CP-201129	0001		B	SIP based subscribe/notify procedures for configuration management	16.1.0
2020-06	CT-88e	CP-201129	0002	1	F	Removal of Editor's notes.	16.1.0
2020-06	CT-88e	CP-201129	0003		F	Corrections in HTTP request-uri value	16.1.0
2020-06	CT-88e	CP-201129	0004		B	Adding IANA registration template for VAL user profile and UE configuration document	16.1.0
2020-06	CT-88e	CP-201129	0005		F	Using proper element names in VAL UE Configuration	16.1.0
2020-09	CT-89e	CP-202163	0006		D	Removing Heading level-7 as per drafting rules	16.2.0
2021-09	CT-93e	CP-212138	0007	1	C	add VAL UE Information to configuration management procedure	17.0.0
2021-12	CT-94e	CP-213052	0008	1	B	Addition of functional entity requirements for CoAP support	17.1.0
2021-12	CT-94e	CP-213052	0009	-	B	Authenticated identity in CoAP request	17.1.0
2021-12	CT-94e	CP-213052	0010	1	B	Addition of CoAP event subscription procedures	17.1.0
2021-12	CT-94e	CP-213052	0011	1	B	Addition of CoAP notifications procedure	17.1.0
2021-12	CT-94e	CP-213052	0012	1	B	Addition of CoAP VAL user profile data procedures	17.1.0
2021-12	CT-94e	CP-213052	0013	2	B	Addition of CoAP Update VAL user profile data procedures	17.1.0
2021-12	CT-94e	CP-213052	0014	1	B	Addition of CoAP resource representation and encoding	17.1.0
2022-03	CT-95e	CP-220255	0015	2	B	Data types applicable to multiple resource representations	17.2.0
2022-03	CT-95e	CP-220255	0016	2	B	Addition of CoAP VAL UE configuration data procedures	17.2.0
2022-03	CT-95e	CP-220255	0017	-	F	Minor corrections in VAL user profile data procedures	17.2.0
2022-03	CT-95e	CP-220255	0018	-	B	Media type for user profile document	17.2.0
2022-03	CT-95e	CP-220255	0019	-	B	Resolving Editor's Note on CoAP use of cache	17.2.0
2022-03	CT-95e	CP-220255	0020	2	F	Corrections in CoAP Resource representation and APIs for VAL user profile	17.2.0
2022-03	CT-95e	CP-220255	0021	3	B	Addition of CoAP Resource representation and APIs for UE configuration	17.2.0
2022-03	CT-95e	CP-220255	0022	-	F	Correction of CR implementation issues	17.2.0
2022-03	CT-95e	CP-220255	0023	-	B	Corrections in Update VAL user profile data procedures	17.2.0
2022-03	CT-95e	CP-220255	0024	-	B	Updates in VAL user profile data SCM server CoAP procedure	17.2.0

History

Document history		
V17.2.0	July 2022	Publication