ETSI TS 124 546 V16.2.0 (2020-10)

5G;
Configuration management - Service Enabler Architecture Layer for Verticals (SEAL);
Protocol specification
(3GPP TS 24.546 version 16.2.0 Release 16)

Reference
RTS/TSGC-0124546vg20

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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".

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 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.

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 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.

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.

6.2.2 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.

6.2.2.2 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.

6.2.3 VAL UE configuration data

6.2.3.1 Client 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; 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].

6.2.3.2 Server 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*".

6.2.4 VAL user profile data

6.2.4.1 Client 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 Server 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.

6.2.5 Update VAL user profile data

6.2.5.1 Client 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 Server 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*".

6.3 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.

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 (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

History

Document history		
V16.1.0	August 2020	Publication
V16.2.0	October 2020	Publication