**3GPP TSG-CT WG1 Meeting #138-eC1-225998r1**

**E-Meeting, 10th – 14th October 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | 24.548 terms alignment and some editorial changes | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Mobile | | | | | | | | | |
| ***Source to TSG:*** | CT1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSEAL | | | | |  | ***Date:*** | | | 2022-09-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Several different terms with the same meaning are used in TS24.548, e.g. SEAL network resource management client and SEAL Network Resource Management Client. This CR is proposed to solve this issue. “Network Resource Management Client” and “Network Resource Management Server” is used for the SNRM-C and SNRM-S respectively; and “network resource management client”/“network resource management server” is used for the related capability/functionality.  Some editorial changes are also proposed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 24.548 terms alignment  Backwards compatibility analysis:  The change doesn’t impact the behaviors or signallings. Thus there is no backwards compatible issue based on the change of this CR. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Different terms with the same meaning are used in TS24.548. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.2, 6.2.1.2, 6.2.2.2.2, 6.2.2.3.1, 6.2.2.3.2, 6.2.3.9.2, 6.2.4, 6.2.4.2.1, 6.2.4.2.3, 6.2.4.2.4, 6.2.4.3.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 1\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

BM-SC Broadcast-Multicast Service Centre

SNRM-C SEAL Network Resource Management Client

SNRM-S SEAL Network Resource Management Server

PCF Policy Control Function

SEAL Service Enabler Architecture Layer for Verticals

VAL Vertical Application Layer

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 2\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 6.2.1.2 Authenticated identity in CoAP request

Upon receiving a CoAP request, the SNRM-S shall authenticate the identity of the sender of the CoAP request as specified in 3GPP TS 24.547 [9], and if authentication is successful, the SNRM-S shall use the identity of the sender of the CoAP request as an authenticated identity.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 3\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.2.2.2 Server procedure

Upon receiving an HTTP POST request message containing:

a) an Accept header field set to "application/vnd.3gpp.seal-unicast-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-unicast-info +xml"; and

c) an application/vnd.3gpp.seal-unicast-info+xml MIME body with a <request> element in the <unicast-info> root element;

the SNRM-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 to request unicast resource, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps; and

2) shall support handling an HTTP POST request from a VAL server according to procedures specified in IETF RFC 4825 [19] "POST Handling"; and

b) shall evaluate the need for network resources and use of resource sharing, and then send a SIP MESSAGE request containing request for resources according to procedures specified in 3GPP TS 29.214 [12] for EPS and/or 3GPP TS 29.514 [14] for 5GS.

Upon receiving a SIP 200 (OK) response to the SIP MESSAGE request, the SNRM-S:

a) shall generate an HTTP 200 (OK) response message according to IETF RFC 7231 [22]. In the HTTP 200 (OK) response message, the SNRM-S:

1) shall include a Request-URI set to the URI corresponding to the identity of the VAL server;

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

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

i) shall include a <request-result> element set to "success" indicating success of the resource request operation; and

b) shall send the HTTP 200 (OK) response message towards the VAL server according to IETF RFC 7231 [22].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 4\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.2.3.1 VAL server procedure

To modify unicast bearers, the VAL server shall generate an HTTP POST request according to procedures specified in IETF RFC 7231 [22]. In the HTTP POST request message, the VAL server:

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

b) shall include an Accept header field set to "application/vnd.3gpp.seal-unicast-info+xml";

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

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

1) shall include a <modification> element which shall include:

i) a <requester-identity> element set to the identity of the VAL server performing the request;

ii) an <identity> element set to the identity of the VAL user or VAL UE which requests the VAL service communication; and

iii) an <requirement-info> element set to the modified unicast resource information; and

e) shall send the HTTP POST request message towards the VAL server according to IETF RFC 7231 [22].

NOTE: Before terminating connection due to no response from the SNRM-S, the VAL server allows sufficient time for the SNRM-S to reserve resources and respond. It is up to implementation to decide how long the VAL server waits for receiving response.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 5\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.2.3.2 Server procedure

Upon receiving an HTTP POST request message containing:

a) an Accept header field set to "application/vnd.3gpp.seal-unicast-info+xml";

b) a Content-Type header field set to "application/vnd.3gpp.seal-unicast-info +xml"; and

c) an application/vnd.3gpp.seal-unicast-info+xml MIME body with a <modification> element in the <unicast-info> root element;

the SNRM-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 to modify unicast resource, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps; and

2) shall support handling an HTTP POST request from a VAL server according to procedures specified in IETF RFC 4825 [19] "POST Handling";

b) if the media bearer modification is not required, shall generate an HTTP 200 (OK) response message according to IETF RFC 7231 [22]. In the HTTP 200 (OK) response message, the SNRM-S:

1) shall include a Request-URI set to the URI corresponding to the identity of the VAL server;

2) shall include a Content-Type header field set to "application/vnd.3gpp.seal-unicast-info+xml";

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

i) shall include a <modification-result> element set to "failure" indicating failure of the resource modification request operation; and

4) shall send the HTTP 200 (OK) response message towards the VAL server according to IETF RFC 7231 [22]; and

c) if the media bearer modification is required, shall send a SIP MESSAGE request containing the modified parameters of the unicast bearer according to procedures specified in 3GPP TS 29.214 [12] for EPS and/or 3GPP TS 29.514 [14] for 5GS.

Upon receiving a SIP 200 (OK) response to the SIP MESSAGE request, the SNRM-S:

a) shall generate an HTTP 200 (OK) response message according to IETF RFC 7231 [22]. In the HTTP 200 (OK) response message, the SNRM-S:

1) shall include a Request-URI set to the URI corresponding to the identity of the VAL server;

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

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

i) shall include a <modification-result> element set to "success" indicating success of the resource modification request operation; and

b) shall send the HTTP 200 (OK) response message towards the VAL server according to IETF RFC 7231 [22].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 6\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.3.9.2 SNRM server HTTP and CoAP procedures

Upon receiving an HTTP POST request message containing:

a) a Content-Type header field set to "application/vnd.3gpp.seal-mbms-usage-info +xml"; and

b) an application/vnd.3gpp.seal-mbms-usage-info+xml MIME body with a <request> element in the <mbms-info> root element;

the SNRM-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 to request mbms resource, shall respond with a HTTP 403 (Forbidden) response to the HTTP POST request and shall skip rest of the steps; and

2) shall support handling an HTTP POST request from a VAL server according to procedures specified in IETF RFC 4825 [19] "POST Handling"; and

b) shall determine to activate MBMS bearer, and then send an MBMS bearer announcement message as described in clause 6.2.3.2.2 or in clause 6.2.3.2.3 towards the SNRM-C.

Upon receiving an MBMS bearer response from the SNRM-C as specified in clause 6.2.3.2.2 or in clause 6.2.3.2.3, the SNRM-S shall send an MBMS bearers response message as specified in clause 6.2.3.2.2 or in clause 6.2.3.2.3 towards the VAL server.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 7\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.2.4 Network assisted UE-to-UE communications resource management

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 8\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.4.2.1 SNRM client HTTP procedure

In order to initiate the network assisted QoS management for UE communications, the SNRM-C shall send an HTTP POST request message according to procedures specified in IETF RFC 7231 [7]. In the HTTP POST request message, the SNRM-C:

a) shall set the Request-URI to the URI identifying the SNRM-S;

b) shall include an Accept header field set to "application/vnd.3gpp.seal-network-QoS-managment-info+xml";

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

d) shall include an application/vnd.3gpp.seal-network-QoS-managment-info+xml MIME body with the <network-QoS-management-info> root element including the <QoS-management-initiation-request> element which:

1) shall include a <VAL-ue-id> element set to the identity or IP address of the SNRM-C acting as the VAL UE and performing the request;

2) shall include a <VAL-ue-list> element with one or more <VAL-ue-id> child elements set to the identities of the VAL UEs which are nodes for the end-to-end application within the VAL service, for which the end-to-end QoS management applies;

3) may include a <VAL-service-id> element set to the VAL service identity of the VAL application;

4) may include <end-to-end-QoS-requirements> element set to the QoS requirements for latency, throughput, reliability and jitter for the VAL application for the end-to-end session;

5) may include a <service-area> element set to the geographical area or topological area where an end-to-end QoS management request applies; and

6) may include a <validity-period> element set to the period of time during which an end-to-end requirement is valid.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 9\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.4.2.3 SNRM client CoAP procedure

In order to initiate the network assisted QoS management for UE communications, the SNRM-C shall create a QoS Session resource by sending a CoAP POST request to the SNRM-S. In the CoAP POST request, the SNRM-C:

a) shall set the CoAP URI to the QoS Sessions resource URI to according to the resource definition in clause A.2.1.2.2.2:

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

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

c) shall include "QosSession" object:

1) shall set "requiredQoS" attribute to the required end-to-end QoS requirement;

2) shall include a list of VAL UEs which are requested to participate in the QoS session in the "participants" attribute, and for each participant, shall add a "SessionParticipant" object in which:

i) shall set "id" attribute to the VAL UE ID; and

ii) if the participant object represents the requesting VAL UE, shall include the "state" object and set its "active" attribute to "true"; and

3) may include "valServiceId" attribute set to the identity of the VAL service enabled by the QoS session;

4) may include one or more geographical area identifiers in "serviceArea" attribute; and

5) may include "validPeriod" attribute set to the time period when the QoS session is valid; and

d) shall send the request protected with the relevant ACE profile (OSCORE profile or DTLS profile) as described in 3GPP TS 24.547 [9].

Upon receiving a CoAP 2.01 (Created) response, the SNRM-C shall store the newly created QoS Session and shall check if it contains a reporting configuration to be applied.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 10\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.4.2.4 SNRM server CoAP procedure

Upon reception of a CoAP POST request where the CoAP URI of the request identifies the QoS Sessions resource URI according to the resource definition in clause A.2.1.2.2.2, the SNRM-S:

a) shall determine the identity of the sender of the received CoAP POST request as specified in clause 6.2.1.X, and:

1) if the identity of the sender of the received CoAP POST request is not authorized to create the QoS session, shall respond with a 4.03 (Forbidden) response to the CoAP POST request and skip rest of the steps;

b) shall support handling an CoAP POST request from a SNRM-C according to procedures specified in IETF RFC 7252  [23]; and

c) shall create a new Individual QoS Session resource and for each VAL UE in the list of participants shall create a new Individual Session Participant resource and shall return a CoAP 2.01 (Created) response with the "QosSession" object including its resource URI in "resUri" attribute, and optionally a reporting configuration in "reportConf" attribute.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Change 11\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 6.2.4.3.4 SNRM server CoAP procedure

Upon reception of a CoAP PUT request where the CoAP URI of the request identifies Individual QoS Session Participant resource as described in clause A.2.1.2.4.3.2, the SNRM-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 QoS session participant resource, 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 SNRM-C according to procedures specified in IETF RFC 7252  [23]; and

c) shall update the individual QoS session participant resource pointed at by the CoAP URI with the content of "SessionParticipant" object received in the request and return a CoAP 2.04 (Changed) response; and

d) if reported QoS is included in "reportedQoS" attribute, shall determine any needed actions to fulfill the end-to-end QoS for the QoS session.