RADISYS ENGAGE MEDIA SERVER™
Containerized Decomposed Media Server User Guide

RELEASE CD18.0.1

February 2023 **007-04984-0000**

PART 1: PRODUCT OVERVIEW

Chapter 1

Product Description

This chapter provides a high-level overview of the Containerized Decomposed Media Server functions, listing key features and components, and providing standards and compliance information.

Key Features

The Containerized Decomposed Media Server can be used in a broad range of applications and services, as follows:

- Decomposed architecture
- AnnLab for clip management
- Audio and multimedia announcement servers
- Call center
- Calling card and prepaid calling card
- IP Centrex or Hosted PBX
- Class 4 or Class 5 switching
- Voice, Web, and video conference
- Interactive Voice Response (IVR) or Voice Response Unit (VRU)
- Voicemail and Videomail
- Unified messaging
- Online gaming
- Transcoding
- Ringback tones
- Push-to-talk
- Lawful Intercept (LI)
- High Complexity (HC) Video
- Codec High Watermark

The Containerized Decomposed Media Server provides the following media resource functions.

- Audio codecs, including G.711 A-law, G.711 µ-law, G.722, G.729A, G.729AB, AMR, AMRWB, OPUS (NB and WB), EVS (NB, WB, and SWB), EVRC-A, EVRC-B, EVRC-NW, Telephone-event, CN (G.711 comfort noise), and RED (RFC 2198 RTP redundancy for AMR or AMR-WB only)
- Video codecs including H.264 (Mode 0 and Mode 1) and VP8
- T.140 text codec

- G.711 and T.38 fax[1] codecs
- Voice-Quality Enhancements
  - Packet Loss Concealment (PLC)
  - Acoustic Echo Cancellation (AEC)
  - Noise Reduction (NR)
  - Noise Gating (NG)
  - Noisy-Line Detection (NLD)
  - R-factor (Rating factor)
- RTCP and RTCP-XR
- Secure RTP Control Protocol (SRTCP)
- RTCP feedback messages including RTCP-PLI, RTCP-FIR, RTCP-TMMBR, and GENERIC-NACK
- Automatic transcoding between different audio and video codec types and bit rates for conferencing, port recording, announcements, and playback of audio announcements
- In-band and RFC 2833 Dual Tone Multi Frequency (DTMF) detection, collection, and generation, including optional DTMF clamping. The Containerized Decomposed Media Server also supports receiving RFC 4733 DTMF-long duration events and multiple events. The Containerized Decomposed Media Server sends out DTMF out-of-band events as per RFC 2833.
- Fixed and variable announcements
- Automatic Speech Recognition (ASR) and Text To Speech (TTS)
- Multilingual announcements (44 languages and dialects[2])
- Tones or announcements, stored inside the Containerized Decomposed Media Server or on the external Network File System (NFS), the Real Time Streaming Protocol (RTSP), Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS) servers
- Recording and playback of audio to internal Containerized Decomposed Media Server memory, NFS, and HTTP/HTTPS servers
- Rich audio mixing and conferencing capabilities suitable for simple conferencing applications, such as residential 3-way calling, to complex business conferencing applications
- Personalized audio stream mixing
- Cascade conferences to increase the number of talk-listen participants
- Flexible gain control including automatic gain control, muting, and unmuting
- HC H.264 and VP8 multimedia announcement and recording features, including announcements with HC text and icon overlay

---

1. Fax on the Containerized Decomposed Media Server is not fully qualified.
2. For information on supported Containerized Decomposed Media Server languages, refer to *Sets and Variables Interface Reference*.

- HC Video conferencing with Voice Activated Switching (VAS) or split-screen continuous presence
- Audio and audio-video media replication for lawful intercept applications
- Fax send and receive
- Call progress analysis for outgoing calls

All the footprint configuration can be performed through the Helm chart. For information on CPU, memory, DSP core, and persistent storage of each component, refer to the *Containerized Decomposed Media Server Installation Guide*.

Containerized Decomposed Media Server in the Network

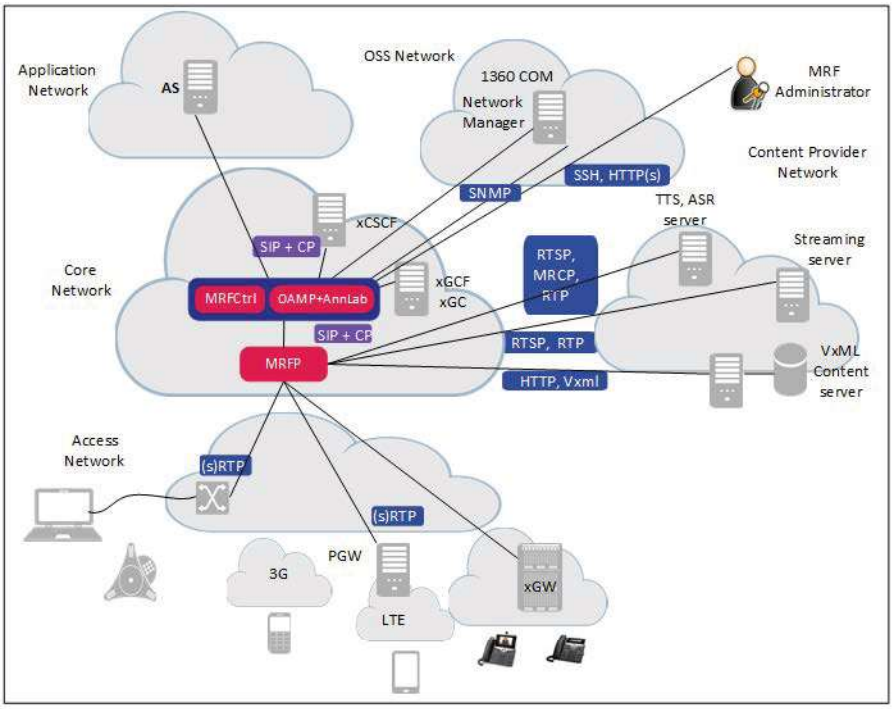
The Radisys Containerized Decomposed Media Server is a carrier-class platform designed from the outset to efficiently and cost-effectively process voice, video, and data, and to combine these into a rich, multi-service communications experience.

Containerized Decomposed Media Server is a flavor of Virtual Network Function (VNF) based Decomposed Media Server. Containerized Decomposed Media Server supports similar functionalities of Decomposed Media Server but developed as a native cloud application and is deployed on carrier-grade Kubernetes deployment. Containerized Decomposed Media Server includes MRFCtrl pod, operations, administration, maintenance, and provisioning (OAMP) pod, and multiple MRFP pods.

The Containerized Decomposed Media Server has a key role in the converged network where subscribers using multimedia enabled PCs, mobile phones, PDAs, and other terminals can communicate seamlessly with one another and with legacy devices in natural and rich multimedia interactions.

Figure 1 shows a high-level view of the network architecture that enables seamless voice and video communications and uniform access to services by all subscribers regardless of their access network and terminal capabilities.

Figure 1. Containerized Decomposed Media Server in IP Network



Composition

The following are the decomposed components (pods) of Containerized Decomposed Media Server.

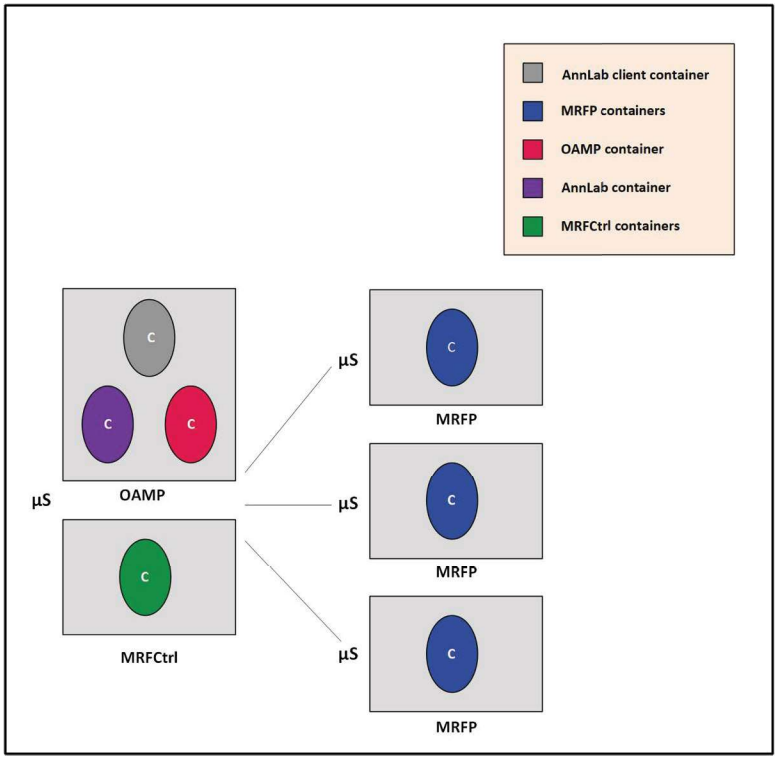
- **MRFCtrl pod.** The SIP endpoint for Containerized Decomposed Media Server and contains single container MRFCtrl.
- **OAMP pod.** This pod contains the following containers.
  - **OAMP container.** Hosts the Containerized Decomposed Media Server GUI and database for configuration. This container is also responsible for all the management activities of the deployment.
  - **AnnLab.** Hosts the AnnLab server that is responsible for clips deployment. In this document, the AnnLab refers to an AnnLab server.
  - **AnnLab Client.** Hosts the AnnLab Client that is responsible for transcoding the clips.
- **MRFP pod.** Responsible for media processing. A variable number of MRFP pods can be launched. However, Containerized Decomposed Media Server supports a maximum of 10 MRFP pods.

Hereafter in this document, the MRFC refers to OAMP and MRFCtrl pod.

NOTE: Each pod consists of a sidecar container to forward logs to Kubernetes.

Figure 2 provides the logical view of Containerized Decomposed Media Server.

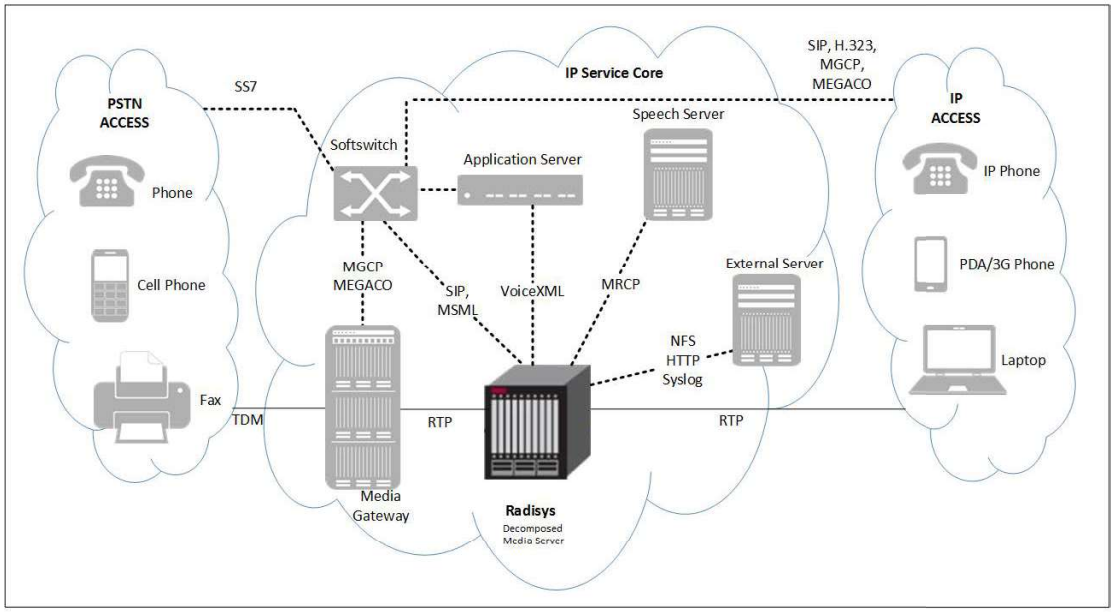
Figure 2. Logical View of Containerized Decomposed Media Server



Third Party Call Control (3PCC) Architecture

The Containerized Decomposed Media Server resides in an IP network as part of an integrated Voice over IP (VoIP) media network. Figure 3 shows the general topology of this network.

Figure 3. Containerized Decomposed Media Server as 3rd Party Call Control



The Containerized Decomposed Media Server is a slave device, which accepts commands and requests from control agents, and communicates with other key elements of the network, such as media gateways, terminals, or a combination of elements.

Containerized Decomposed Media Server Redundancy

The Containerized Decomposed Media Server offers the following redundancy features.

- 1+1 (active/standby) redundancy for MRFCs
- N+k (active/active) redundancy for MRFPs without call preservation
- N+1 (where N ≤ 5) redundancy for MRFPs with call preservation

MRFCtrl Redundancy

The MRFCtrl pod includes MRFCtrl and sidecar containers for logs. Use a keepalived daemon to maintain MRFCTRL High Availability (HA). Both the MRFCtrl pods are in *Running state* and keepalived monitors the status. Based on the state, one of the MRFCtrl have MRFCTRL VIP, and the MRFCtrl process gets started on that pod. Two MRFCtrl pod instances are launched, namely, mrfctrl-0 and mrfctrl-1. The keepalived daemon runs as the root user in both the pods.

Execute the following commands to get the state of the current pod.

```
[root@master dmrf]# kubectl exec -n <namespace> -it mrf-mrfctrl-0 -c mrfctrl cat
/opt/swms/etc/status
STATE="BACKUP"
[root@master dmrf]# kubectl exec -n <namespace> -it mrf-mrfctrl-1 -c mrfctrl cat
/opt/swms/etc/status
STATE="MASTER"
[root@master dmrf]#
```

MRFP N+k Redundancy

The Containerized Decomposed Media Server supports N+k (active/active) MRFP redundancy for MRFPs without call preservation. That is, N MRFP pods handle the load of N+k MRFPs when k instances are unreachable or out of service. In N+k redundancy, the optimal value is determined for N and k so that Containerized Decomposed Media Server is not overloaded when a certain number of MRFP pods (k) are not handling the calls.

MRFP N+1 Redundancy

The Containerized Decomposed Media Server supports MRFP pod redundancy with multiple redundancy groups, and each group with a maximum of N+1 (where N ≤ 5) MRFPs with call preservation for MSML, MSCML, and Netann conferences.

For more information on MRFP redundancy support, see *MRFP N+1 Redundancy on page 156*.

Interfaces

The Containerized Decomposed Media Server uses the following interfaces to communicate over the network.

- **SIP, VoiceXML, MSML, MSCML, MOML.** The Containerized Decomposed Media Server receives commands and responds to requests from control agents using open control protocols such as SIP, VoiceXML, Media Sessions Markup Language (MSML), Media Server Control Markup Language (MSCML), and Media Objects Markup Language (MOML).
- **RTP.** The Containerized Decomposed Media Server sends and receives Real Time Protocol (RTP) streams over a media network to and from RTP endpoints, where an endpoint can be an IP-capable terminal or a media gateway. This interface is used for media sessions, IVR, DTMF collection and generation, and playing media clips.
- **SRTP and SRTCP.** The Containerized Decomposed Media Server sends and receives Secure RTP (SRTP) streams over a media network to and from SRTP-capable endpoints. Secure RTP Control Protocol (SRTCP) is supported for monitoring the flow of SRTP packets.
- **RTCP, RTCP-XR, RTCP-PLI, RTCP-FIR, TMMBR/TMMBN, and Generic-NACK.** The Containerized Decomposed Media Server sends and receives RTP Control Protocol (RTCP) packets used for monitoring the flow of RTP packets. It sends Sender Report (SR), Receiver Report (RR), Source Description (SDES), and BYE packets, and receives SR, RR, and BYE packets. It also supports a number of RTCP Extended Report (RTCP-XR) statistics and RTCP

Picture Loss Indication (RTCP-PLI) messages to indicate picture loss in the media session. The Containerized Decomposed Media Server supports RTCP-FIR I-frame request capability for video sessions. Temporary Maximum Media Bit-rate Request (TMMBR) and Temporary Maximum Media Bitrate Notification (TMMBN) messages are used for dynamic video rate adaptation as required by IR.941 for terminals supporting video. Generic-NACK (RTCP-NACK) messages are used for notification and retransmission of the lost RTP video packets.

- **Web-enabled GUI.** An HTTP/HTTPS Web-based GUI allows system administrators to perform GUI configuration for the Containerized Decomposed Media Server.
- **SNMP.** All the Containerized Decomposed Media Server configurations and functions can be performed through a Simple Network Management Protocol (SNMP) interface. The Containerized Decomposed Media Server supports SNMP versions 2c and 3.
- **NFS.** The Containerized Decomposed Media Server can record media clips, and play them back, from an external NFS server.
- **HTTP/HTTPS.** The Containerized Decomposed Media Server can stream audio or audio-video clips to an external HTTP or HTTPS server and store them in a persistent file. The Containerized Decomposed Media Server can also playback audio clips using streamed mode and audio-video clips using cache mode, stored on an external HTTP or HTTPS server. The Containerized Decomposed Media Server supports HTTP or HTTPS recording for both port and conference. The Containerized Decomposed Media Server can also retrieve VoiceXML files from an HTTP or HTTPS server for processing, and return results to the server. The Containerized Decomposed Media Server includes the Server Name Indication (SNI) extension header as per RFC 6066 when communicating with the HTTPS remote server for announcement, recording, file transfer, fax-recv, and fax-send operations. For HTTP, these processes are managed by a control agent and no special configuration of Containerized Decomposed Media Server is required. Whereas, the HTTPS requires certificate configuration, see *Manage Certificates on page 323*.
- **MRCP (Version 1 and Version 2).** The Containerized Decomposed Media Server uses Media Resource Control Protocol (MRCP) to access speech resources on external servers. These resources include speech recognizers for ASR and speech synthesizers for TTS.
- **RTSP.** The Containerized Decomposed Media Server streams announcement from an RTSP server. Additionally, RTSP is supported as required by MRCP Version 1 for an ASR or TTS client device.
- **DNS.** The Containerized Decomposed Media Server uses Domain Name System (DNS) to resolve domain names for IP addresses.
- **NETCONF.** The Containerized Decomposed Media Server supports Network Configuration (NETCONF) protocol for configuration and management functions. The Containerized Decomposed Media Server supports SSH version 2 for exchanging the NETCONF message with the client. For more information on NETCONF, refer the *NETCONF Interface Reference*.

- **X3 Interface.** The Containerized Decomposed Media Server supports lawful intercept of Call Content (CC) over the X3 interface. In order to support lawful intercept of the CC, an application server named Lawful Intercept Function (LIF) is used. LIF invokes the Containerized Decomposed Media Server through the establishment of a related series of SIP dialogs.

  The sip:monitor is used as a service indicator to create pass-through dialogs and listener dialogs within the lawful intercept group. The Containerized Decomposed Media Server allows to create a maximum of five listener dialogs for each pass-through ports in a sip:monitor LI group. In mono mode, both the listener audio medias must have the same IP address and port number.

  The Containerized Decomposed Media Server supports sip:monitor service indicator for lawful intercept of the fax media type. The Containerized Decomposed Media Server supports CC interception on the image (fax) port in stereo mode. The Containerized Decomposed Media Server receives and transmits the fax packets over User Datagram Protocol Transport Layer (UDPTL), on both pass-through port and listener port. The Containerized Decomposed Media Server pass-through the fax packet from one party to another without any modification, except for modifying the IP and UDP layer to include the Containerized Decomposed Media Server IP address or port as the source, and peer party IP address or port as the destination.

  In the stereo mode, the Containerized Decomposed Media Server replicates and forwards the fax packet to LIG in two RTP streams without any modification, except for the IP and UDP layer changes to include the Containerized Decomposed Media Server IP address or port as the source, and LIG IP address or port as the destination.

  For more information refer to the *SIP Interface Reference*.

Protocol Standard Compliance

This section describes the standards supported by the Containerized Decomposed Media Server.

Table 1. Network Communications Protocol Standards

Protocol	Standard
ARP	RFC 826
DNS	• RFC 1034, RFC 1035 • RFC 3596 (IPv6)
DiffServ/ToS	RFC 2474
Ethernet	IEEE 802.3
IP Version 4 (IPv4)	RFC 791

Table 1. Network Communications Protocol Standards

Protocol	Standard
IP Version 6 (IPv6)	• RFC 2460 Internet Protocol Version 6 (IPv6) Specification • RFC 3493 (socket extension) • RFC 4291 (addressing architecture) • RFC 2464 (transmission) • RFC 4862 (auto-configuration for link-local addresses) • RFC 4861 (neighbor discovery) • RFC 4443 (ICMPv6) • RFC 1981 (MTU discovery) • RFC 3484 (default address selection) • RFC 4604 (IGMPv3) • RFC 4213 (dual-stack transition mechanism)
TCP	RFC 793 RFC 4145 (Media Control Channel Framework TCP channel)
UDP	RFC 768
TLS[a]	• RFC 2246 (TLSv1.0) • RFC 4346 (TLSv1.1) • RFC 5246 (TLSv1.2)
TLS extension	RFC 6066 (Server Name Indication)
DTLS	RFC 6347 and 4347
DTLS extension	RFC 5763 and 5764

[a] MRFP supports all the TLS versions TLSv1.0, TLSv1.1, and TLSv1.2; whereas MRFCtrl and OAMP Pod supports only the TLSv1.2 version.

Table 2. Control Protocol Standards

Protocol	Standard
MRCP	RFC 4463 Informational
MSML and MOML	RFC 5707
MSCML	RFC 5022
SDP	• RFC 3264 (Offer/Answer Model) • RFC 4566

Table 2. Control Protocol Standards

Protocol	Standard
SIP	• RFC 2543, RFC 2543bis04 • RFC 2976 (INFO Method) • RFC 3261, RFC 2543bis04 • RFC 3261 • RFC 3262 (100Rel) • RFC 3312 • RFC 3263 (locating SIP servers) • RFC 3264 • RFC 3326 (reason header) • RFC 3581 • RFC 3725 • RFC 4028 (session timer) • RFC 4092 (alternative network address types) • RFC 4240 • RFC 4412 (resource priority) • Early Media • RFC 6230 (media control channel framework)
SRGS	As specified in the W3C GRXML file format
VoiceXML 2.0	W3C Candidate Recommendation Version 2 (March 2004)
VoiceXML 2.1	W3C Recommendation 19 (June 2007)

Table 3. Management Protocol Standards

Protocol	Standard
DiffServ	RFC 2475
HTTP v1.0 HTTP v1.1	RFC 1945 RFC 2616
HTTPS	RFC 2818
NFS v3	RFC 1094
SNMP v2 plus support for community strings (SNMPv2c)	• RFC 1901–1908 • RS-232: RFC 1659 • IP: RFC 2011 • Interfaces: RFC 2233
LDAP	• RFC 4616 • RFC 2247 • RFC 2307bis • RFC 822

Table 3. Management Protocol Standards

Protocol	Standard
SNMPv3	• RFC 3411–3418 • RFC 2574 User-based Security Model (USM) • RFC 1213 MIB-II • RFC 3411 SNMP-FRAMEWORK-MIB • RFC 3412 SNMP-MPD-MIB • RFC 3413 SNMP-TARGET-MIB • RFC 3414 SNMP-USER-BASED-SM-MIB • RFC 3415 SNMP-VIEW-BASED-ACM-MIB • RFC 3416 SNMPv2-PDU
NETCONF	RFC 6241

Table 4. Media Protocol Standards

Protocol	Standard
AMR, AMR-WB	• RFC 4867 3GPP Adaptive Multi-Rate (Octet-aligned and bandwidth efficient) • 3GPP TS 26.171, 3GPP TS 26.190-26.194, 3GPP TS 26.201
RTCP-PLI	RFC 4585 (PLI only)
RTCP-FIR	RFC 5104
RTCP-TMMBR/TMMBN	RFC 5104
RTCP-NACK	RFC 4585
H.264 Mode 0 and Mode 1	• ITU H.264 Video Codec, also known as Advanced Video Codec (AVC) • RFC 6184, previously RFC 3984 • Constrained Baseline Profile Level 1.1b, 1.1, 1.2, 1.3, 2, 2.1, 2.2, 3, and 3.1
H.265	• ITU H.265 Video Codec, also known as High Efficiency Video Codec (HEVC) • RFC 7798 • Main Profile Level 1, 2, 2.1, 3, and 3.1
ITU-T E.180/Q.35	ITU-T Recommendation E.180/Q.35 (March 1998)
ITU G.711 u-law and A-law	• RFC 3551 (PCMU and PCMA) • ITU-T G.711 Appendix I
CN	• RFC 3389 (PCMU and PCMA) • ITU-T G.711 Appendix II
ITU G.722	• RFC 3551 (G.722) • ITU G.722 Appendix IV
ITU G.729 and Annexes A, B	• RFC 3551 • ITU G.729 Annexes A and B
ITU-T Q.1970 3GPP TS 29.414	BICC IP Bearer Control Protocol (IPBCP)
ITU-T T.30	ITU-T Recommendation T.30 (April 1999)
ITU-T T.38	ITU-T Recommendation T.38 (April 2007)
ITU-T V.21	ITU-T Recommendation V.21 (November 1988)
RED	RFC 2198 for AMR, AMR-WB, and T.140 (text)

Table 4. Media Protocol Standards

Protocol	Standard
RTT	• RFC 4103 (RTP payload for text conversation) • draft-ietf-avtcore-multi-party-rtt-mix-11 (RTP-mixer formatting of multiparty Real-Time Text)
RTP	• RFC 3550 • RFC 4961 • RFC 4867 • RFC 3611 (RTCP-XR)
RTSP	RFC 2326 as required for MRCP Version 1
BUNDLE (RTP Media Multiplexing)	RFC 5888
RTSP	RFC 2326 as required for MRCP Version 1
SRTP	RFC 3711
In-band DTMF Detection Standard	• EIA/TIA-464A • GR-181CORE • ITU-T Q.24
Telephone Events	RFC 4733 with some exceptions[a]
Telephone Events	RFC 2833/ RFC 4733
VP8	RFC 6386
Opus	draft-ietf-payload-rtp-opus or RFC 6716 Opus speech and audio codec
EVS	Standardized by 3GPP (3Q2014). 3GPP TS 26.441 - 3GPP TS 26.451[b]
EVRC, EVRCB, and EVRCNW EVRC0, EVRCB0, and EVRCNW0	• 3GPP2 C.S0014-A service option 3, 3GPP2 C.S0014-B service option 68, 3GPP2 C.S0014-D service option 73 • RFC 3588, RFC 5188, RFC 6884
SDP	RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams

[a] Long DTMF digits: The Containerized Decomposed Media Server detects each segment (of long digit) as new digit and the Containerized Decomposed Media Server cannot generate a digit longer than 8.19s. Multiple events in single packet: The Containerized Decomposed Media Server would detect only the first digit in a packet and ignore all subsequent digits in a packet. Transmission of state events indicated by event duration of zero: The Containerized Decomposed Media Server does not check the duration of the first packet, so it will not interpret received event as a state event. The Containerized Decomposed Media Server sends RFC 2833 events with non-zero duration in the first packet.

[b] The Containerized Decomposed Media Server does not support 3GPP TS 26.448.