International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.5002

(12/2019)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Signalling requirements and protocols for IMT-2020 – Signalling requirements and architecture of IMT-2020

Signalling requirements and architecture for media service entity attachment

Recommendation ITU-T Q.5002

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
Signalling requirements and architecture of IMT-2020	**Q.5000–Q.5019**
Protocols for IMT-2020	Q.5020–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.5002

Signalling requirements and architecture for media service entity attachment

Summary

Media service providers for different service technologies have always developed independently in order to satisfy the requirements of their platform. This creates various different verticals, which leads to significant drawbacks and inefficiencies in terms of development. Media service providers using cloud capability have to deal with specific signalling flows for providing media service using an interface, which will significantly increase the complexity for the provider to use different cloud infra providers. Therefore, there is a strong necessity for requirements and architecture for a standard signalling convergence of different cloud infra providers in future media services.

Recommendation ITU-T Q.5002 specifies the signalling requirements and architecture for media service entity attachment. This Recommendation mainly describes high level signalling requirements and specific requirements for media infra layer, media service layer, application programming interface (API) layer and orchestration layer.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.5002	2019-12-14	11	11.1002/1000/14146

Keywords

Cloud computing, media entities, media platform, media service, signalling architecture, signalling requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T Q.5002

Signalling requirements and architecture for media service entity attachment

1 Scope

This Recommendation specifies signalling requirements and architecture for attachment of media services which consist of media functional entities. It describes the following:

– Signalling architecture for attachment of media service entities.

– Signalling requirements to attach media service entities for the relevant layers: media application programming interface (API) layer, media processing layer, media delivery layer, media infra abstraction layer and media orchestration layer.

– Security considerations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

3 Definitions

None.

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 media service: A service providing the electronic communication tools that are used to store, aggregate, share, discuss and deliver various types of content.

3.1.5 resource management [b-ITU-T Y.3520]: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 media service entity: A service functional entity that provides live and video on demand (VoD) media services with capabilities such as encoding, decoding, storage, content delivery and caching.

3.2.2 media as a service (MaaS): A cloud service category that provides the cloud service customer with the ability to attach, configure compose, manage and deliver media service functions.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

CDN Content Delivery Network

CRUD Create Read Update Delete

DASH Dynamic Adaptive Streaming over HTTP

DB Database

DRM Digital Rights Management

FE Functional Entity

HLS HTTP Live Streaming

HTTP Hypertext Transfer Protocol

IGMP Internet Group Management Protocol

IPTV Internet Protocol Television

MaaS Media as a Service

MAL Media API Layer

MPL Media Processing Layer

MDL Media Delivery Layer

MIAL Media Infra Abstraction Layer

MOL Media Orchestration Layer

OTT Over the Top

URL Uniform Resource Locator

VoD Video on Demand

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

Future media platforms will accommodate various types of devices which belong to service providers. In addition, there are a lot of technologies using the cloud to provide media services to increase user satisfaction.

Media service providers for different service technologies have always developed independently in order to satisfy the requirements of their platform. This creates various different verticals, which leads to significant drawbacks and inefficiencies in terms of development. Media service providers using cloud capability have to deal with specific signalling flows for providing media service using an interface, which will significantly increase the complexity for the provider to use different cloud computing providers.

Therefore, there is strong necessity for requirements and architecture for a signalling convergence of different cloud computing providers in future media services, as shown in Figure 6-1.

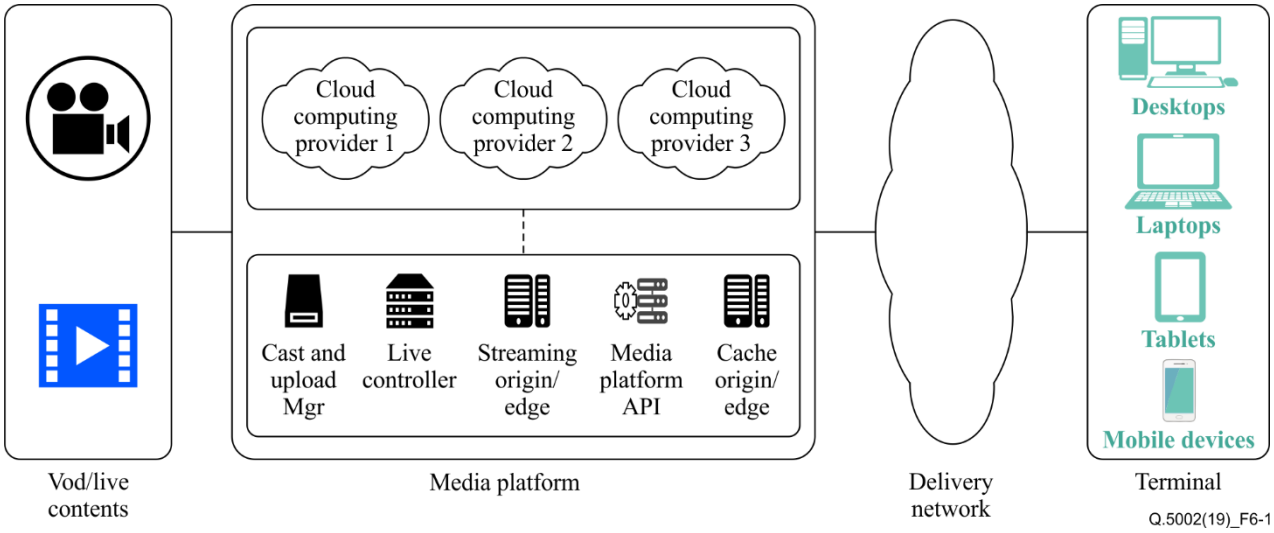

Figure 6-1 – Overall architecture for media service entity attachment

7 Signalling architecture

7.1 Signalling architectural model for media service entity attachment

Figure 7-1 shows an architectural model for media service entity attachment which provides an overall layering model for media services and applications with sets of media functional entities.

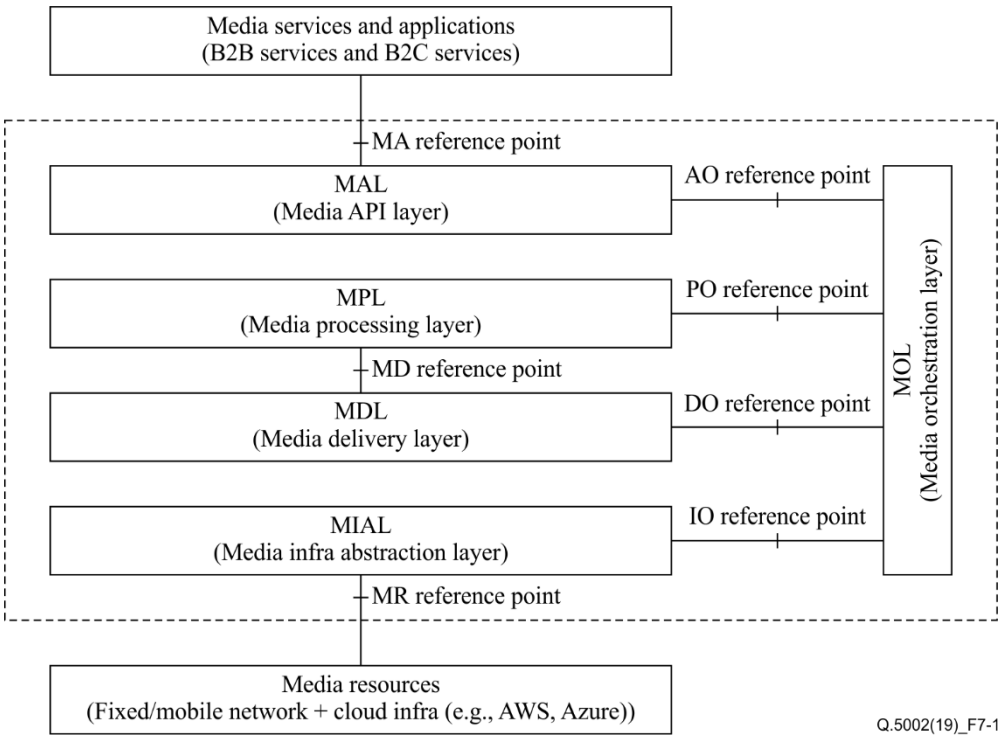

Figure 7-1 – Architectural model for media service entity attachment

7.2 Media services and applications

Media services and applications provide various media related services and applications such as mobile IPTV, fixed IPTV, OTT, etc.

7.3 MEDIA API layer

The media API layer (MAL) provides application program interfaces to interconnecting media related functional entities which are described in the media processing layer (MPL), media delivery layer (MDL), media infra abstraction layer (MIAL) and media orchestration layer (MOL). Figure 7-2 shows the architectural model for the media API layer (MAL).

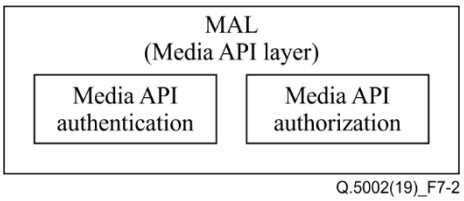

Figure 7-2 – Architectural model for media API layer

7.3.1 Media API Authentication FE

The Media API Authentication functional entity (FE) provides a process for identifying users when media services and applications want to use the services of media as a service (MaaS).

7.3.2 Media API Authorization FE

The Media API Authorization FE provides a procedure for checking whether a user is authorized to use the application programming interface (API). It also establishes and ensures a security mechanism that allows different APIs to be used to query and list available APIs according to the level of privilege.

7.4 Media processing layer

The media processing layer (MPL) provides functionalities which are required for media processing tasks. There are predefined media processing functional entities (Fes) as shown in Figure 7-3.

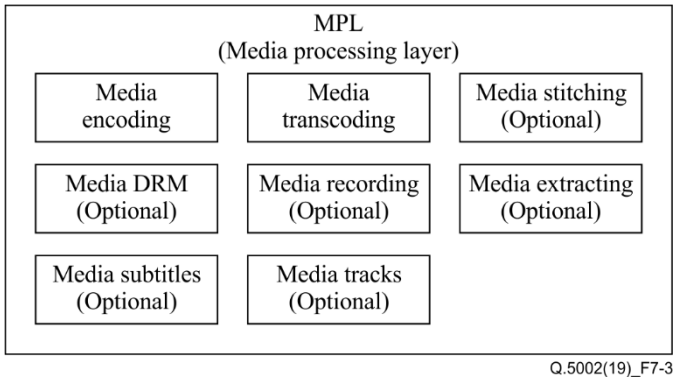

Figure 7-3 – Architectural model for media processing layer (MPL)

7.4.1 Media Encoding FE

The Media Encoding FE provides a process of converting a given video input into a digital format that is compatible with various media players. Each video format comes with its own specifications such as video codecs (H264, H265, Webm, etc.) and audio codec (MP3, AAC, etc.)

7.4.2 Media Transcoding FE

The Media Transcoding FE provides media codec conversion that changes a video format from one to another, to make videos viewable across different platforms and devices.

7.4.3 Media Stitching FE

The Media Stitching FE provides the process of combining multiple media sources (e.g., video and images) with overlapping fields of view to produce a segmented 360 degree videos or panorama medias.

7.4.4 Media DRM FE

The Media DRM FE protects the media content by preventing leakage of the original content from the content server to the end user.

7.4.5 Media Recording FE

The Media Recording FE can record live channels and store them on a separate storage, which can provide a search function and provide a function to reproduce video on demand (VOD) contents.

7.4.6 Media Extracting FE

The Media Extracting FE provides a function to extract a specific image of a movie and use it as a thumbnail image or a preview image.

7.4.7 Media Subtitle FE

The Media Subtitle FE provides the function of uploading the subtitle of the media in a separate file so that it can be transmitted together with the moving picture.

7.4.8 Media Multi Tracks FE

The Media Multi Tracks FE provides users with the function to select audio tracks encoded in different national languages or audio tracks encoded with different codecs and sound effects.

7.5 Media delivery layer

The Media delivery layer (MDL) provides functionalities which are required media delivery tasks. There are predefined media delivery functional entities as shown in Figure 7-4.

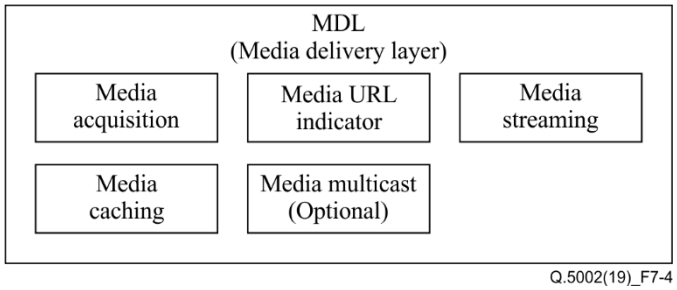

Figure 7-4 – Architectural model for media delivery layer (MDL)

7.5.1 Media Acquisition FE

The Media Acquisition FE allows the user to input basic information about the content when the media file is input to the system, and the information is automatically registered in the database (DB). The content source is delivered to a predetermined location in the storage, and the location information of the content is registered together with the DB.

7.5.2 Media URL Indicator FE

The Media URL Indicator FE provides the function of delivering the location of the media file or the uniform resource locator (URL) of the location to be transmitted

7.5.3 Media Streaming FE

The Media Streaming FE provides a process of delivering media (e.g., video, audio, etc.) to play the media before the end-user obtains the entire file for the content.

7.5.4 Media Caching FE

The Media Caching FE stores media for the future contents requests so that media can be served faster; the media stored in a cache might be the result of an earlier requested, or preloaded media stored in cache servers.

7.5.5 Media Multicast FE

The Media Multicast FE provides group communication where data transmission is addressed to a group of destinations (e.g., IPv4 class D, eMBMS, etc.). Multicast can be one-to-many or many-to-many distribution and can be joined by group management protocols such as Internet group mManagement protocol (IGMP).

7.6 Media infra abstraction layer

Figure 7-5 shows the architectural model for the media infra abstraction layer (MIAL) and associated FEs.

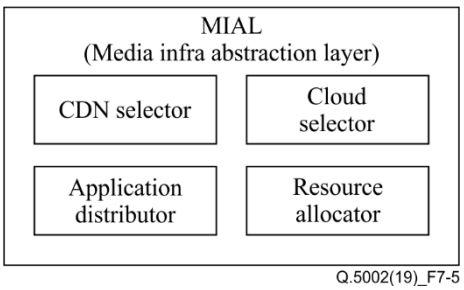

Figure 7-5 – Architectural model for media infra abstraction layer (MIAL)

7.6.1 CDN Selector FE

The CDN Selector FE supports the function to select and service a variety of 3rd party content delivery networks (CDNs).

7.6.2 Cloud Selector FE

The Cloud Selector FE supports the function to select from a variety of 3rd party cloud services.

7.6.3 Application Distributor FE

The Application Distributor FE provides the function to pre-work and automatically deploy multiple applications in each layer to the destination server or cluster.

7.6.4 Resource Allocator FE

The Resource Allocator FE provides the ability to scale the various cloud resources.

7.7 Media orchestration layer

Figure 7-6 shows the architectural model for media orchestration layer (MOL) and associated Fes.

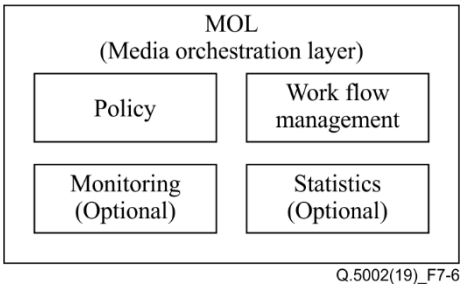

Figure 7-6 – Architectural model for media orchestration layer (MOL)

7.7.1 Policy FE

The Policy FE provides functions to create and manage policies that can manage processing, delivery and infrastructure.

7.7.2 Work Flow Management FE

The Work Flow Management FE provides the function to connect functions required from contents acquisition to distribution and manage them by the service unit.

7.7.3 Monitoring FE

The Monitoring FE provides functions to monitor the status of services such as media processing, delivery, infrastructure and service status.

7.7.4 Statistics FE

The Statistics FE provides functions such as collecting, analyzing and visualizing various statistical data obtained from media processing, delivery and infrastructure.

7.8 Reference points

7.8.1 Reference point MA

The reference point MA is between the media service and applications and the media API layer. This reference point is used to request API list information provided by MaaS from the media API layer and to give the information to applications. This reference point is also used to request the API access list that the requesting media service is acquiring, access control information acquired for each API and the authorization for each API.

7.8.2 Reference point MD

The reference point MD is between the MPL and the MDL. This reference point allows the MPL and the MDL to interact for requesting information of the media delivery list.

7.8.3 Reference point MR

The reference point MR is between the MIAL and media resources. This reference point is used to request information on the media source list in use.

7.8.4 Reference point AO

The reference point AO is between the MAL and the MOL. This reference point allows the MAL and the MOL to interact for requesting media policy and configuration in the MAL.

7.8.5 Reference point PO

The reference point PO is between the MPL and the MOL. This reference point allows the MPL and the MOL to interact for requesting policy and configuration on media processing in the MPL.

7.8.6 Reference point DO

The reference point DO is between the MDL and the MOL. This reference point allows the MDL and the MOL to interact for requesting policy and configuration on media delivery in the MDL.

7.8.7 Reference point IO

The reference point IO is between the MIAL and the MOL. This reference point allows the MIAL and the MOL to interact for requesting policy and configuration in order to service interworking of media infra abstraction.

8 Signalling requirements

8.1 Signalling requirement for reference point MA (Application-MAL)

MA is required to query and execute the API provided by the MAL.

MA is required to deliver event notifications received from the MOL.

8.2 Signalling requirement for reference point MD (MPL-MDL)

MD is required to transfer codec information (stream ID, codec profiles) provided by the MPL to the MDL.

MD is required to transfer streaming information (stream ID, IP address, domain, streaming protocol) provided by the MDL to the MPL.

MD is required to deliver event notifications that occur in the MPL or the MDL.

8.3 Signalling requirement for reference point MR (MIAL-Media resources)

MR is required to query and execute the API provided by each media resource.

MR is required to quire media resources information (location, resource capacity, usage) of each media resource.

MR is required to deliver event notifications that occur in each media resource.

8.4 Signalling requirement for reference point AO (MAL-MOL)

8.4.1 Contents management

AO is required to create, read, update and delete media contents.

8.4.2 Cloud management

AO is required to query public cloud information such as location, price, capacity and usage.

AO is required to select public cloud service.

8.5 Signalling requirement for reference point PO (MPL-MOL)

PO is required to transfer streaming information (IP address, domain, stream ID, protocol) needed to communicate with the MDL.

PO is required to create, read, update and delete MPL resources.

PO is required to query MPL information such as capacity, usage and profile.

PO is required to transfer API to create, read, update and delete media resource received from the MIAL to the MPL.

PO is required to deliver event notifications that occur in MPL

8.6 Signalling requirement for reference point DO (MDL-MOL)

DO is required to transfer streaming information such as IP address, domain, stream ID and protocol needed to communicate with the MPL.

DO is required to create, read, update and delete MDL resources.

DO is required to query MDL information such as capacity, usage and protocol.

DO is required to transfer API to create / read / update /delete media resource received from the MIAL to the MPL.

DO is required to deliver event notifications that occur in the MDL.

8.7 Signalling requirement for reference point IO (MIAL-MOL)

IO is required to transfer abstracted API can be used by MPL and MDL

IO is required to query media resource information (resource name, location, capacity, usage)

IO is required to deliver event notifications that occur in each media resource.

9 MEA procedures and signalling description

9.1 Signalling flow and message for reference point MA (Applications-MAL)

It exists between media applications and the MAL to exchange signalling message for requesting API list information provided by MaaS. In addition, the application needs to request the access control information acquired for each API and the authorization for each API. The protocol used at

the MA reference point can be Restful, Web service, etc. Figure 9-1 shows signalling flows for reference point MA.

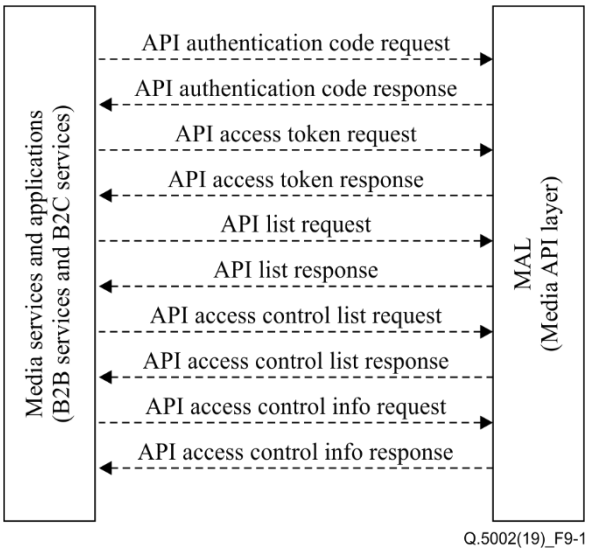

Figure 9-1 – Signalling flows for reference point MA

9.1.1 API authentication code request and response message

The API authentication code message is defined as API-AUTHENTICATION-CODE message. This message is sent by the application to the MAL for requesting the API authentication (*CRUD) code.

9.1.1.1 API authentication code request

The API authentication code request information flow is sent by applications to the MAL to obtain the authentication code. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< MA-API-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-API-Version }

{ MA-API-Name }

{ MA-API-Description}

{ MA-API-Argument-Info }

{ Service-Name, Authority(CRUD) }

9.1.1.2 API authentication code response

The API authentication code response information flow is sent by the MAL to applications to provide the authentication code. It contains the following information components:

Message format:

< MA-API-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-Response-Code }

{ MA-Response-Message}

{ MA-API-Result }

{ API-Authentication-Code }

9.1.2 API access token request and response message

The API access token message is defined as API-ACCESS-TOKEN message. This message is sent by the application to the MAL for requesting the API access token.

9.1.2.1 API access token request

The API access token request information flow is sent by applications to the MAL to obtain the API access token. It contains the following information components:

Message format:

< MA-API-ACCESS-TOKEN-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-API-Version }

{ MA-API-Name }

{ MA-API-Description }

{ MA-API-Argument-Info }

{ Authentication-Code }

9.1.2.2 API access token response

The API access token response information flow is sent by the MAL to applications to provide the API access token. It contains the following information components:

Message format:

< MA-API-ACCESS-TOKEN-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-Response-Code }

{ MA-Response-Message}

{ MA-API-Result }

{ API-Access-Token }

9.1.3 API list request and response message

The API list information message is defined as API-LIST message. The API-LIST message, indicated by the message type in the message header field, is sent by the application to the MAL to request the API list information provided by MaaS and then the MAL responds to the application through the response message with the required API list information.

9.1.3.1 API list request

The API list request information flow is sent by applications to the MAL to obtain the API list information. It contains the following information components:

Message format:

< MA-API-LIST-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-API-Version }

{ MA-API-Name }

{ MA-API-Description }

{ MA-API-Argument-Info }

{ Entity-ID or Service-ID }

{ Access-Token }

9.1.3.2 API list response

The API list response information flow is sent by the MAL to applications to provide the API list information. It contains the following information components:

Message format:

< MA-API-LIST-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-Response-Code }

{ MA-Response-Message }

{ MA-API-Result }

{ API-ID#1, API-Name, Description }

{ API-ID#N, API-Name, Description }

9.1.4 API access control list request and response message

The API access control list message is defined as API-ACCESS-CONTROL-LIST message. The API-ACCESS-CONTROL-LIST message is sent by the application to the MAL for requesting the API access control list information.

9.1.4.1 API access control list request

The API access control list request information flow is sent by applications to the MAL to obtain the API access list information. It contains the following information components:

Message format:

< MA-API-ACCESS-CONTROL-LIST-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-API-Version }

{ MA-API-Name }

{ MA-API-Description}

{ MA-API-Argument-Info }

{ Entity-ID or Service-ID },

{ Access-Token }

9.1.4.2 API access control list response

The API access control list response information flow is sent by MAL to applications to provide the API access control list information. It contains the following information components:

Message format:

< MA-API-ACCESS-CONTROL-LIST-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-Response-Code }

{ MA-Response-Message}

{ MA-API-Result }

{ API-ID#1, API-Name, Description, API-Access-Control-Type(CRUD) },

{ API-ID#N, API-Name, Description, API-Access-Control-Type(CRUD) }

9.1.5 API access control info request and response message

The API access control message is defined as API-ACCESS-CONTROL-INFO message. The API-ACCESS-CONTROL-INFO message is sent by the application to the MAL for requesting the API access control information.

9.1.5.1 API access control info request

The API access control info request information flow is sent by applications to the MAL to obtain the API access info information. It contains the following information components:

Message format:

< MA-API-ACCESS-CONTROL-INFO-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-API-Version }

{ MA-API-Name }

{ MA-API-Description}

{ MA-API-Argument-Info }

{ Entity-ID or Service-ID }

{ Access-Token }

9.1.5.2 API access control info response

The API access control info response information flow is sent by the MAL to applications to provide the API access control information. It contains the following information components:

Message format:

< MA-API-ACCESS-CONTROL-INFO-Message> ::= < Message Header >

{ MA-Request-ID }

{ MA-Response-Code }

{ MA-Response-Message }

{ MA-API-Result }

{ API-ID, API-Name, Description, Request-Count(Total, Used, Remained) }

9.2 Signalling flow and message for reference point MD (MPL-MDL)

It exists between the MPL and the MDL interact for requesting information of media delivery list. The MPL requests streaming information to the MDL and also the MPL sends streaming information such as stream ID, IP address, domain and streaming protocol to the MPL. Figure 9-2 shows signalling flows for reference point MD.

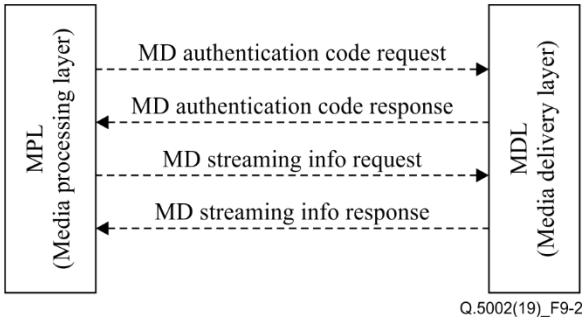

Figure 9-2 – Signalling flows for reference point MD

9.2.1 MD authentication code request and response message

The MD authentication code message is defined as MDI-AUTHENTICATION-CODE message. This message is sent by the MPL to the MDL for requesting the MD authentication (*CRUD) code.

9.2.1.1 MD authentication code request

The MD authentication code request information flow is sent by the MPL to the MDL to obtain the MD authentication code information. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< MD-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MD-Request-ID }

{ MD-API-Version }

{ MD-API-Name }

{ MD-API-Description }

{ MD-API-Argument-Info }

{ Service-ID, Authority(CRUD) }

9.2.1.2 MD authentication code response

The MD authentication code response information flow is sent by the MDL to the MPL to provide the MD authentication code. It contains the following information components:

Message format:

< MD-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MD-Request-ID }

{ MD-Response-Code }

{ MD-Response-Message }

{ MD-API-Result }

{MD-Authentication-Code }

9.2.2 MD streaming info request and response message

The MD streaming information message is defined as MD-STREAMING-INFO-CODE message. The MD-STREAMING-INFO-CODE message is sent by the MPL to the MDL for requesting the streaming information such as streaming ID, IP address, domain and streaming protocol provided from MDL and then the MDL response to the MPL through the response message with the required MD streaming information.

9.2.2.1 MD streaming info request

The MD streaming info request information flow is sent by the MPL to the MDL to obtain the MD streaming information. It contains the following information components:

Message format:

<MD-STREAMING-INFO-Message> ::= < Message Header >

{ MD-Request-ID }

{ MD-API-Version }

{ MD-API-Name }

{ MD-API-Description }

{ MD-API-Argument-Info }

{ MD-Authentication-Code }

{ Entity-ID or Service-ID }

9.2.2.2 MD streaming info response

The MD streaming info request information flow is sent by the MDL to the MPL to provide the MD streaming information. It contains the following information components:

Message format:

<MD-STREAMING-INFO-Message> ::= < Message Header >

{ MD-Request-ID }

{ MD-Response-Code }

{ MD-Response-Message }

{ MD-API-Result }

{ MD-Codec-Info }

{ MD-Streaming-Info }

9.3 Signalling flow and message for reference point MR (MIAL-Media Resources)

It exists between MIAL and media resources to interact for requesting information of media resources. MIAL requests media resources information such as location, resource capacity and usage to media resources and also media resources sends media resources information such as provider, location, resource capacity, usage to the MIAL. Figure 9-3 shows signalling flows for reference point MR.

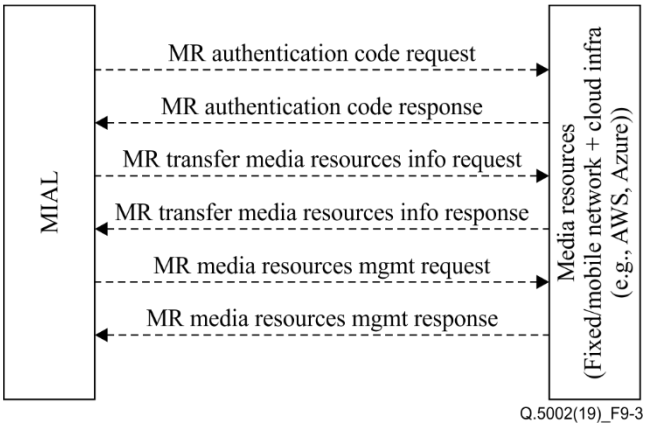

Figure 9-3 – Signalling flows for reference point MR

9.3.1 MR authentication code request and response message

The MR authentication code message is defined as MR-AUTHENTICATION-CODE message. This message is sent by the MIAL to the media resources for requesting the MR authentication (*CRUD) code.

9.3.1.1 MR authentication code request

The MR authentication code request information flow is sent by the MIAL to media resources to obtain the MR authentication code information. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< MR-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MR-Request-ID }

{ MR-API-Version }

{ MR-API-Name }

{ MR-API-Description }

{ MR-API-Argument-Info }

{ Service-ID, Authority(CRUD) }

9.3.1.2 MR authentication code response

The MR authentication code request information flow is sent by media resource to the MIAL to obtain the MR authentication code. It contains the following information components:

Message format:

< MR-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ MR-Request-ID }

{ MR-Response-Code }

{ MR-Response-Message }

{ MR-API-Result }

{MR-Authentication-Code }

9.3.2 MR media resource management request and response message

The MR media resource management message is defined as MR-MEDIA-RESOURCE-MGMT-CODE message. The MEDIA-RESOURCE-MGMT message is sent by the MIAL to the media resources for managing the media resources and then the media resources response to the MIAL through the response message with the required media resources information such as provider, location, resource capacity and usage.

9.3.2.1 MR media resources management request

The MR media resource management request information flow is sent by the MIAL to media resources to obtain the MR media resource management information such as location, resource capacity and usage. It contains the following information components:

Message format:

<MR-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ MR-Request-ID }

{ MR-API-Version }

{ MR-API-Name }

{ MR-API-Description }

{ MR-API-Argument-Info }

{ MR-Authentication-Code }

{ Media-Resource-ID }

9.3.2.2 MR media resources management response

The MR media resource management request information flow is sent by media resources to the MIAL to provide the media resource management information. It contains the following information components:

Message format:

<MR-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ MR-Request-ID }

{ MR-Response-Code }

{ MR-Response-Message }

{ MR-API-Result }

{ MR-Media-Resources-Info }

9.4 Signalling flow and message for reference point AO (MAL-MOL)

It exists between the MAL and the MOL to interact for managing media contents. The MAL sends requests to manage media contents and requesting cloud information to the MOL. The MOL sends status of media contents and cloud information such as location, price, capacity, usage to the MAL. Figure 9-4 shows signalling flows for reference point AO.

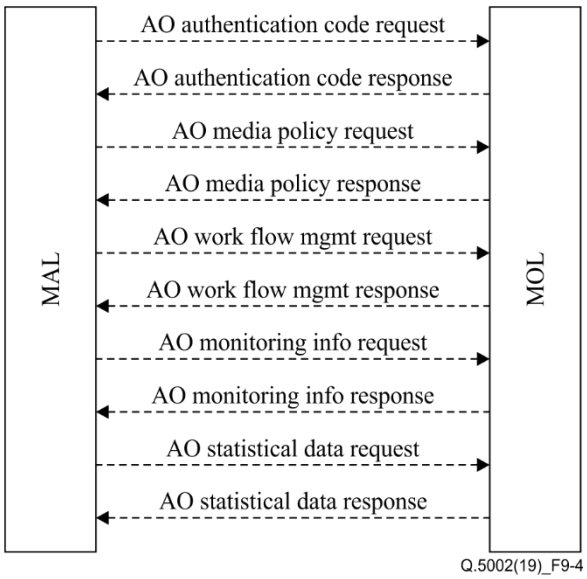

Figure 9-4 – Signalling flows for reference point AO

9.4.1 AO authentication code request and response message

The AO authentication code message is defined as AO-AUTHENTICATION-CODE message. This message is sent by the MAL to the MOL for requesting the AO authentication (*CRUD) code.

9.4.1.1 AO authentication code request

The AO authentication code request information flow is sent by the MAL to the MOL to obtain the AO authentication code. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< AO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-API-Version }

{ AO-API-Name }

{ AO-API-Description }

{ AO-API-Argument-Info }

{ Service-ID, Authority(CRUD) }

9.4.1.2 AO authentication code response

The AO authentication code request information flow is sent by the MOL to the MAL to provide the authentication code. It contains the following information components:

Message format:

< AO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-Response-Code }

{ AO-Response-Message }

{ AO-API-Result }

{ AO-Authentication-Code }

9.4.2 AO media policy request and response message

AO media policy message is defined as AO-MEDIA-POLICY-CODE-Message. The MEDIA-POLICY message is sent by the MAL to the MOL for requesting media policy such as profile, codec and then MOL response to the MAL through the response message with the required media policy information.

9.4.2.1 AO media policy request

The AO media policy request information flow is sent by the MAL to the MOL to obtain the media policy information. It contains the following information components:

Message format:

< AO-MEDIA-POLICY-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-API-Version }

{ AO-API-Name }

{ AO-API-Description }

{ AO-API-Argument-Info }

{ AO-Authentication-Code }

{ Media-Policy-Entity-ID }

9.4.2.2 AO media policy response

The AO media policy request information flow is sent by the MOL to the MAL to provide the media policy information. It contains the following information components:

Message format:

< AO-MEDIA-POLICY-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-Response-Code }

{ AO-Response-Message }

{ AO-API-Result }

{ AO-Media-Policy-Info }

9.4.3 AO work flow management request and response message

The AO work flow management message is defined as AO-WORKFOLW-MGMT-Message. The WORKFLOW-MGMT message is sent by the MAL to the MOL for managing service flow such as stream ingest-transcoding-packetizing-delivery or combination of each job and then the MOL responds to the MAL through the response message with the required work flow information.

9.4.3.1 AO work flow management request

The AO work flow management request information flow is sent by the MAL to the MOL to obtain the work flow management information. It contains the following information components:

Message format:

< AO-WORKFLOW-MGMT-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-API-Version }

{ AO-API-Name }

{ AO-API-Description}

{ AO-API-Argument-Info }

{ AO-Authentication-Code }

{ Workflow-Entity-ID }

9.4.3.2 AO work flow management response

The AO work flow management request information flow is sent by the MOL to the MAL to provide the work flow management information. It contains the following information components:

Message format:

< AO-WORKFLOW-MGMT-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-Response-Code }

{ AO-Response-Message }

{ AO-API-Result }

{ AO-Workflow-Info }

9.4.4 AO monitoring information request and response message

AO monitoring information message is defined as AO-MONITOR-INFO-Message. The MONITOR-INFO message is sent by the MAL to the MOL for requesting monitor information such as usage, capacity and price, then the MOL responds to the MAL through the response message with the required monitoring information or job status.

9.4.4.1 AO monitoring information request

The AO monitoring information request flow is sent by the MAL to the MOL to obtain the monitoring information. It contains the following information components:

Message format:

< AO-WORKFLOW-MGMT-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-API-Version }

{ AO-API-Name }

{ AO-API-Description }

{ AO-API-Argument-Info }

{ AO-Authentication-Code }

{ Monitoring-Entity-ID }

9.4.4.2 AO monitoring information response

The AO monitoring information request flow is sent by the MOL to the MAL to provide the monitoring information. It contains the following information components:

Message format:

< AO-WORKFLOW-MGMT-CODE-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-Response-Code }

{ AO-Response-Message }

{ AO-API-Result }

{ AO-Monitoring-Info }

9.4.5 AO statistical data request and response message

AO statistical data message is defined as AO-STAT-DATA-Message. The STAT-DATA message is sent by the MAL to the MOL for requesting statistical data such as rank, engagement, count, traffic and then MOL response to the MAL through the response message with the required statistical data.

9.4.5.1 AO statistical data request

The AO statistical data request flow is sent by the MAL to the MOL to obtain the statistical data information. It contains the following information components:

Message format:

< AO-STAT-DATA-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-API-Version }

{ AO-API-Name }

{ AO-API-Description }

{ AO-API-Argument-Info }

{ AO-Authentication-Code }

{ Statistical-Data-Entity-ID }

9.4.5.2 AO statistical data response

The AO statistical data request flow is sent by the MOL to the MAL to provide the statistical data information. It contains the following information components:

Message format:

< AO-STAT-DATA-Message> ::= < Message Header >

{ AO-Request-ID }

{ AO-Response-Code }

{ AO-Response-Message }

{ AO-API-Result }

{ AO-Statistical-Data-Info }

9.5 Signalling flow and message for reference point PO (MPL-MOL)

It exists between the MPL and the MOL interacts for managing media contents processing. The MPL sends requesting media resources and transfer streaming information to the MOL. The MOL sends media resources and streaming information received from the MIAL. Also the MOL sends message for managing media contents processing such as encoding and transcoding. Figure 9-5 shows signalling flows for reference point PO.

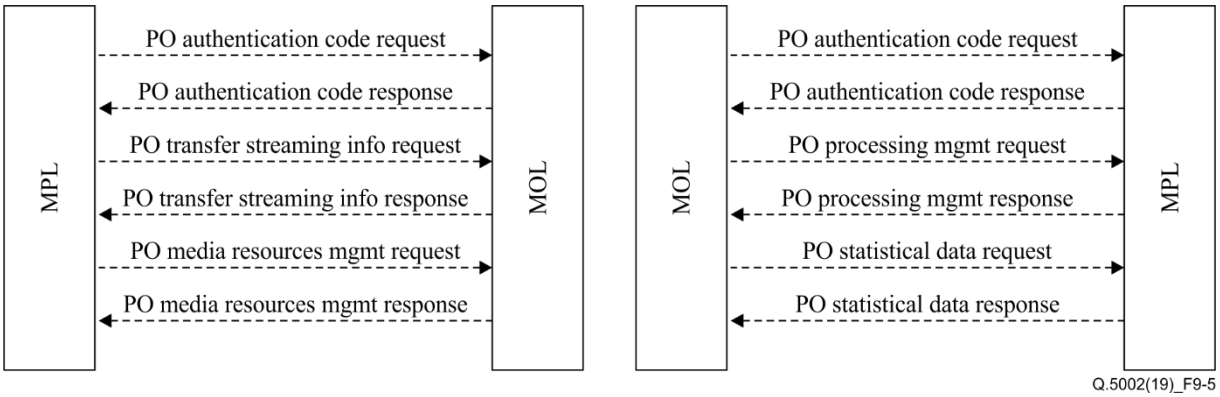

Figure 9-5 – Signalling flows for reference point PO

9.5.1 PO authentication code request and response message

The PO authentication code message is defined as PO-AUTHENTICATION-CODE message. This message is sent by the MPL(MOL) to the MOL(MPL) for requesting the AO authentication (*CRUD) code.

9.5.1.1 PO authentication code request

The PO authentication code request information flow is sent by the MPL(MOL) to the MOL(MPL) to obtain the authentication code. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< PO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-API-Version }

{ PO-API-Name }

{ PO-API-Description }

{ PO-API-Argument-Info }

{ Service-ID, Authority(CRUD) }

9.5.1.2 PO authentication code response

The PO authentication code response information flow is sent by the MOL(MPL) to the MPL(MOL)to provide the authentication code. It contains the following information components:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< PO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-Response-Code }

{ PO-Response-Message }

{ PO-API-Result }

{ PO-Authentication-Code }

9.5.2 PO transfer streaming info request and response message

PO transfer streaming info message is defined as PO-TRANSFER-STREAMING-INFO-Message. The TRANSFER-STREAMING-INFO message is sent by the MPL to the MOL for requesting transfer streaming info such as IP address, domain, stream id, protocol and then MOL response to the MPL through the response message with the required streaming information.

9.5.2.1 PO transfer streaming info request

The PO transfer streaming info request information flow is sent by the MPL to the MOL to obtain the transfer streaming information. It contains the following information components:

Message format:

< PO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-API-Version }

{ PO-API-Name }

{ PO-API-Description }

{ PO-API-Argument-Info }

{ PO-Authentication-Code }

{ Service-ID }

9.5.2.2 PO transfer streaming info response

The PO media resources management response information flow is sent by the MOL(MPL) to the MPL(MOL) to provide the media resources management information. It contains the following information components:

Message format:

< PO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-Response-Code }

{ PO-Response-Message }

{ PO-API-Result }

{ Transfer-Streaming-Info }

9.5.3 PO media resources management request and response message

PO media resources management message is defined as PO-MEDIA-RESOURCES-MGMT-Message. The MEDIA-RESOURCES-MGMT message is sent by the MPL to the MOL for requesting media resources such as IP address, domain, stream id, protocol and then the MOL responds to the MPL through the response message with the required media resources information.

9.5.3.1 PO media resources management request

The PO media resources management request information flow is sent by the MPL(MOL) to the MOL(MPL) to obtain the media resources management information. It contains the following information components:

Message format:

< PO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-API-Version }

{ PO-API-Name }

{ PO-API-Description }

{ PO-API-Argument-Info }

{ PO-Authentication-Code }

{ Media-Resource-ID }

9.5.3.2 PO media resources management response

The PO media resources management response information flow is sent by the MOL(MPL) to the MPL(MOL) to provide the media resources management information. It contains the following information components:

Message format:

< PO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-Response-Code }

{ PO-Response-Message }

{ PO-API-Result }

{ Media-Resource-Info }

9.5.4 PO processing management request and response message

The PO processing management message is defined as PO-PROCESSING-MGMT-Message. The PROCESSING-MGMT message is sent by the MOL to the MPL for requesting media processing job such as encoding/transcoding and then the MPL responds to the MOL through the response message with the required processing status information.

9.5.4.1 PO processing management request

The PO processing management request information flow is sent by the MPL(MOL) to the MOL(MPL) to obtain the processing management information. It contains the following information components:

Message format:

< PO-PROCESSING-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-API-Version }

{ PO-API-Name }

{ PO-API-Description }

{ PO-API-Argument-Info }

{ PO-Authentication-Code }

{ Service-ID}

9.5.4.2 PO processing management response

The PO processing management response information flow is sent by the MOL (MPL) to the MPL(MOL) to provide the processing management information. It contains the following information components:

Message format:

< PO-PROCESSING-MGMT-CODE-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-Response-Code }

{ PO-Response-Message }

{ PO-API-Result }

{ PO-Processing-Job-Info }

{ PO-Processing-status-Info }

9.5.5 PO statistical data request and response message

The PO statistical data message is defined as PO-STAT-DATA-Message. The STAT-DATA message is sent by the MOL to the MPL for requesting statistical data such as capacity, usage and then MPL response to the MOL through the response message with the required statistical data.

9.5.5.1 PO statistical data request

The PO statistical data request flow is sent by the MOL to the MPL to obtain the statistical data information. It contains the following information components:

Message format:

< PO-STAT-DATA-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-API-Version }

{ PO-API-Name }

{ PO-API-Description }

{ PO-API-Argument-Info }

{ PO-Authentication-Code }

{ Service-ID }

9.5.5.2 PO statistical data response

The PO statistical data request flow is sent by the MPL to the MOL to provide the statistical data information. It contains the following information components:

Message format:

< PO-STAT-DATA-Message> ::= < Message Header >

{ PO-Request-ID }

{ PO-Response-Code }

{ PO-Response-Message }

{ PO-API-Result }

{ PO-Statistical-Data-Info }

9.6 Signalling flow and message for reference point DO (MDL-MOL)

It exists between the MDL and the MOL to interact for managing media contents processing. The MDL sends requesting media resources and transfer streaming information to the MOL. The MOL sends media resources and streaming information received from the MIAL. Also the MOL sends message for managing media delivery such as ingest, URL indicator, streaming and caching. Figure 9-6 shows signalling flows for reference point DO.

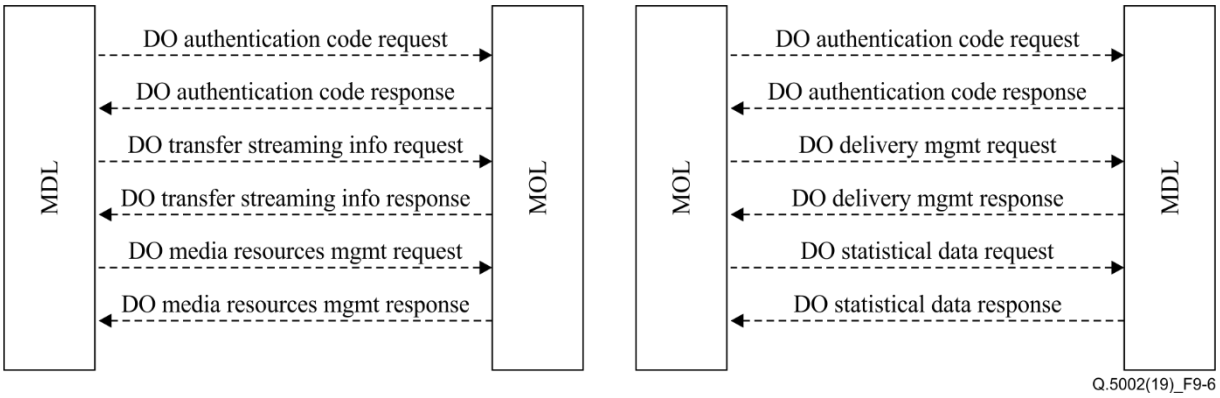

Figure 9-6 – Signalling flows for reference point DO

9.6.1 DO authentication code request and response message

The DO authentication code message is defined as DO-AUTHENTICATION-CODE message. This message is sent by the MDL(MOL) to the MOL(MDL) for requesting the AO authentication (*CRUD) code.

9.6.1.1 DO authentication code request

The DO authentication code request information flow is sent by the MDL(MOL) to the MOL(MDL) to obtain the authentication code. It contains the following information components:

Message format:

*C: Create / R: Read / U: Update / D: Delete

Message format:

< DO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-API-Version }

{ DO-API-Name }

{ DO-API-Description }

{ DO-API-Argument-Info }

{ Service ID, Authority(CRUD) }

9.6.1.2 DO authentication code response

The DO authentication code response information flow is sent by the MOL(MDL) to the MDL(MOL) to provide the authentication code. It contains the following information components:

Message format:

*C: Create / R: Read / U: Update / D: Delete

Message format

< DO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ Service-Session-ID }

{ DO-ID }

{ DO-Name }

{ DO-Description }

{ DO-Argument-Info }

{ Service ID, Authority(CRUD) }

{ DO-Result }

{ DO-Authentication-Code }

9.6.2 DO media resources management request and response message

The DO media resources management message is defined as DO-MEDIA-RESOURCES-MGMT-Message. The DO-MEDIA-RESOURCES-MGMT message is sent by the MDL to the MOL for requesting media resources such as IP address, domain, stream ID, protocol and then the MOL responds to the MDL through the response message with the required media resources information.

9.6.2.1 DO media resources management request

The DO media resources management request information flow is sent by the MDL(MOL) to the MOL(MDL) to obtain the information for media resources management. It contains the following information components:

Message format:

< DO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-Response-Code }

{ DO-Response-Message }

{ DO-API-Result }

{ DO-Authentication-Code }

9.6.2.2 DO media resources management response

The DO media resources management response information flow is sent by the MOL(MDL) to the MDL(MOL) to provide the information for media resources management. It contains the following information components:

Message format:

< DO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ Service-Session-ID }

{ DO-ID }

{ DO-Name }

{ DO-Description }

{ DO-Argument-Info }

{ DO-Authentication-Code }

{ Service ID }

{ DO-Result }

{DO-Media-Resource-Info }

9.6.3 DO transfer streaming info request and response message

DO transfer streaming info message is defined as DO-TRANSFER-STREAMING-INFO-Message. The TRANSFER-STREAMING-INFO message is sent by the MDL to the MOL for requesting transfer streaming info such as IP address, domain, stream id, protocol and then MOL response to the MDL through the response message with the required streaming information.

9.6.3.1 DO transfer streaming info request

The DO transfer streaming info request information flow is sent by the MDL to the MOL to obtain the transfer streaming information. It contains the following information components:

Message format:

< DO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-API-Version }

{ DO-API-Name }

{ DO-API-Description }

{ DO-API-Argument-Info }

{ DO-Authentication-Code }

{ Service-ID }

9.6.3.2 DO transfer streaming info response

The DO media resources management response information flow is sent by the MOL to the MDL to provide the media resources management information. It contains the following information components:

Message format:

< DO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-Response-Code }

{ DO-Response-Message }

{ DO-API-Result }

{ Transfer-Streaming-Info }

9.6.4 DO media resources management request and response message

DO media resources management message is defined as DO-MEDIA-RESOURCES-MGMT-Message. The DO-MEDIA-RESOURCES-MGMT message is sent by the MDL to the MOL for requesting media resources such as IP address, domain, stream ID, protocol and then MOL response to the MDL through the response message with the required media resources information.

9.6.4.1 DO media resources management request

The DO media resources management request information flow is sent by the MDL(MOL) to the MOL(MDL) to obtain the information for media resources management. It contains the following information components:

Message format:

< DO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-API-Version }

{ DO-API-Name }

{ DO-API-Description }

{ DO-API-Argument-Info }

{ DO-Authentication-Code }

{ Media-Resource-ID }

9.6.4.2 DO media resources management response

The DO media resources management response information flow is sent by the MOL(MDL) to the MDL(MOL) to provide the information for media resources management. It contains the following information components:

Message format:

< DO-MEDIA-RESOURCE-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-Response-Code }

{ DO-Response-Message }

{ DO-API-Result }

{ Media-Resource-Info }

9.6.5 DO delivery management request and response message

The DO delivery management message is defined as DO-DELIVERY-MGMT-Message. The DO-DELIVERY-MGMT message is sent by the MOL to the MDL for requesting media delivery job such as ingest, URL indicator, streaming and caching and then the MDL responds to the MOL through the response message with the required delivery job information.

9.6.5.1 DO delivery management request

The DO delivery management request information flow is sent by the MDL(MOL) to the MOL(MDL) to obtain the information for delivery management. It contains the following information components:

Message format:

< DO-DELIVERY-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-API-Version }

{ DO-API-Name }

{ DO-API-Description }

{ DO-API-Argument-Info }

{ DO-Authentication-Code }

{ Media-Delivery-Entity-ID }

9.6.5.2 DO delivery management response

The DO delivery management response information flow is sent by the MOL(MDL) to the MDL(MOL) to provide the information for delivery management. It contains the following information components:

Message format:

< DO-DELIVERY-MGMT-CODE-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-Response-Code }

{ DO-Response-Message }

{ DO-API-Result }

{ Media-Delivery-Info }

9.6.6 DO statistical data request and response message

DO statistical data message is defined as DO-STAT-DATA-Message. The STAT-DATA message is sent by the MOL to the MDL for requesting statistical data such as capacity, usage, protocol and then MDL response to the MOL through the response message with the required statistical data.

9.6.6.1 DO statistical data request

The DO statistical data request flow is sent by the MOL to the MDL to obtain the statistical data information. It contains the following information components:

Message format:

< DO-STAT-DATA-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-API-Version }

{ DO-API-Name }

{ DO-API-Description }

{ DO-API-Argument-Info }

{ DO-Authentication-Code }

{ Service-ID }

9.6.6.2 DO statistical data response

The DO statistical data request flow is sent by the MDL to the MOL to provide the statistical data information. It contains the following information components:

Message format:

< DO-STAT-DATA-Message> ::= < Message Header >

{ DO-Request-ID }

{ DO-Response-Code }

{ DO-Response-Message }

{ DO-API-Result }

{ DO-Statistical-Data-Info }

9.7 Signalling flow and message for reference point IO (MIAL-MOL)

It exists between the MIAL and the MOL interacts for requesting information of media infra. The MOL requests media infra abstraction information to the MIAL and also the MIAL sends media infra abstraction information such as CDN selector, cloud selector, application distribution and resource allocator to the MOL. Figure 9-7 shows signalling flows for reference point IO.

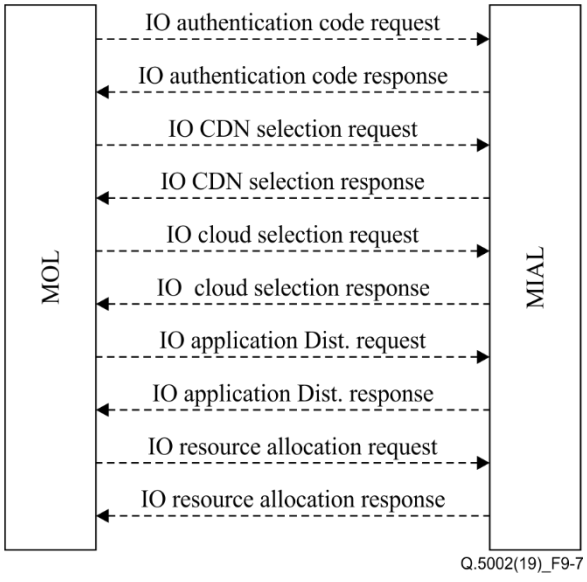

Figure 9-7 – Signalling flows for reference point IO

9.7.1 IO authentication code request and response message

The IO authentication code message is defined as IO-AUTHENTICATION-CODE message. This message is sent by the MOL to the MIAL for requesting the IO authentication (*CRUD) code.

9.7.1.1 IO authentication code request

The IO authentication request information flow is sent by the MOL to the MIAL to obtain the authentication code. It contains the following information components:

Message format:

< IO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-API-Version }

{ IO-API-Name }

{ IO-API-Description }

{ IO-API-Argument-Info }

{ Service ID, Authority(CRUD) }

9.7.1.2 IO authentication code response

The IO authentication response information flow is sent by the MIAL to the MOL to provide the authentication code. It contains the following information components:

Message format:

< IO-AUTHENTICATION-CODE-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-Response-Code }

{ IO-Response-Message }

{ IO-API-Result }

{ IO-Authentication-Code }

9.7.2 IO CDN selection request and response message

The IO CDN selection message is defined as IO-CDN-SELECTION-Message. The IO-CDN-SELECTION message is sent by the MOL to the MIAL for requesting CDN information and then the MIAL responds to the MOL through the responses message with the required CDN provider's information.

9.7.2.1 IO CDN selection request

The IO CDN selection request information flow is sent by the MOL to the MIAL to obtain the CDN selection information. It contains the following information components:

Message format:

< IO-CDN-SELECTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-API-Version }

{ IO-API-Name }

{ IO-API-Description }

{ IO-API-Argument-Info }

{ IO-Authentication-Code }

{ CDN-Selector-Entity-ID }

9.7.2.1 IO CDN selection response

The IO CDN selection response information flow is sent by the MIAL to the MOL to provide the CDN selection information. It contains the following information components:

Message format:

< IO-CDN-SELECTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-Response-Code }

{ IO-Response-Message }

{ IO-API-Result }

{ CDN-Info }

9.7.3 IO cloud selection request and response message

IO cloud selection message is defined as IO-CLOUD-SELECTION-Message. The IO-CLOUD-SELECTION message is sent by the MOL to the MIAL for requesting cloud service information and then MIAL response to the MOL through the response message with the required cloud service providers and provided services information.

9.7.3.1 IO cloud selection request

The IO cloud selection request information flow is sent by the MOL to the MIAL to obtain the cloud selection information. It contains the following information components:

Message format:

< IO-CLOUD-SELECTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-API-Version }

{ IO-API-Name }

{ IO-API-Description }

{ IO-API-Argument-Info }

{ IO-Authentication-Code }

{ Cloud-Selector-Entity-ID }

9.7.3.2 IO cloud selection response

The IO cloud selection response information flow is sent by the MIAL to the MOL to provide the cloud selection information. It contains the following information components:

Message format:

< IO-CLOUD-SELECTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-Response-Code }

{ IO-Response-Message }

{ IO-API-Result }

{ Cloud-Resource-Info }

9.7.4 IO application distribution request and response message

The IO application distribution message is defined as IO-APPLICATION-DISTRIBUTION-Message. The IO-APPLICATION-DISTRIBUTION message is sent by the MOL to the MIAL for requesting cloud and resource information

9.7.4.1 IO application distribution request

The IO application distribution request information flow is sent by the MOL to the MIAL to obtain the information for application distribution. It contains the following information components:

Message format:

< IO-APPLICATION-DISTRIBUTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-API-Version }

{ IO-API-Name }

{ IO-API-Description }

{ IO-API-Argument-Info }

{ IO-Authentication-Code }

{ Application-Distribution-Entity-ID }

9.7.4.2 IO application distribution response

The IO application distribution response information flow is sent by the MIAL to the MOL to provide the information for application distribution. It contains the following information components:

Message format:

< IO-APPLICATION-DISTRIBUTION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-Response-Code }

{ IO-Response-Message }

{ IO-API-Result }

{ Application-Distribution-Info }

9.7.5 IO resource allocation request and response message

The IO resource allocation message is defined as IO-RESOURCE-ALLOCATION-Message. The IO-RESOURCE-ALLOCATION message is sent by the MOL to the MIAL for requesting cloud provider and service information.

9.7.5.1 IO resource allocation request

The IO resource allocation request information flow is sent by the MOL to the MIAL to obtain the information for resource allocation. It contains the following information components:

Message format:

< IO-RESOURCE-ALLOCATION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-API-Version }

{ IO-API-Name }

{ IO-API-Description}

{ IO-API-Argument-Info }

{ IO-Authentication-Code }

{ Resource-Allocator-Entity-ID }

9.7.5.2 IO resource allocation response

The IO resource allocation response information flow is sent by the MIAL to the MOL to provide the information for resource allocation. It contains the following information components:

Message format:

< IO-RESOURCE-ALLOCATION-Message> ::= < Message Header >

{ IO-Request-ID }

{ IO-Response-Code }

{ IO-Response-Message }

{ IO-API-Result }

{ Resource-Allocation-Info }

10 Security considerations

This Recommendation provides signalling architecture and requirements for media service entity attachment based on MaaS environments. Thus, it is assumed that security considerations in general are based on the security framework from cloud computing [b-ITU-T X.1601] and the data security requirements for the monitoring service of cloud computing [b-ITU-T X.1603].

Appendix I

Media service architecture using cloud computing capability

(This appendix does not form an integral part of this Recommendation.)

Bandwidth-intensive media applications have evolved in concert with their supporting delivery platforms and underlying communication infrastructures. There has been a distinct synergy between the requirements of rich media service and value-added networks, architecture, services and technologies. Particularly, as resource constraints on mobile devices have become more relaxed, users have been demanding the same real-time rich media experience on their mobile devices that they get on a PC-like platform. Mobile media traffic has been increasing rapidly and current media traffic (e.g., video, music, etc.) ratio exceeded over 55% in total traffic. Therefore, how to efficiently provide media services is important especially with a focus on scalability. Virtualization technologies could be one solution as most service providers try to extend their infrastructure into the cloud. Figure I.1 shows mobile traffic ratios.

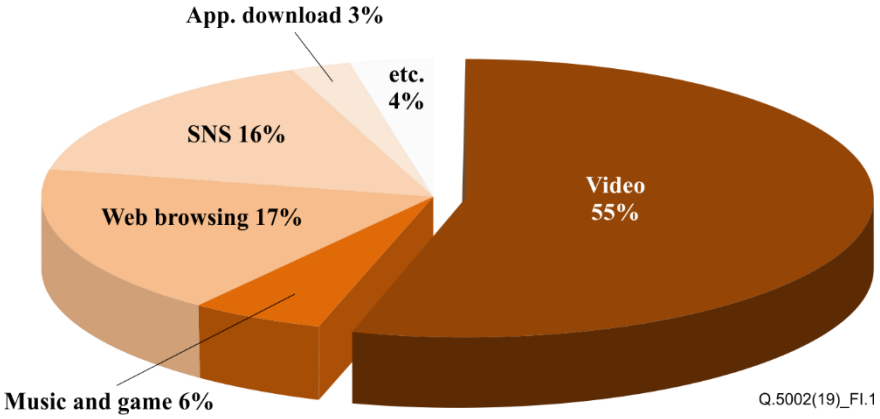

Figure I.1 – Mobile traffic ratio [b-Media Traffic Ratio]

As shown in Figure I.2, current media services need many signalling entities in different locations in networks. Therefore, it is not easy to manage and scale out whenever media traffic increases.

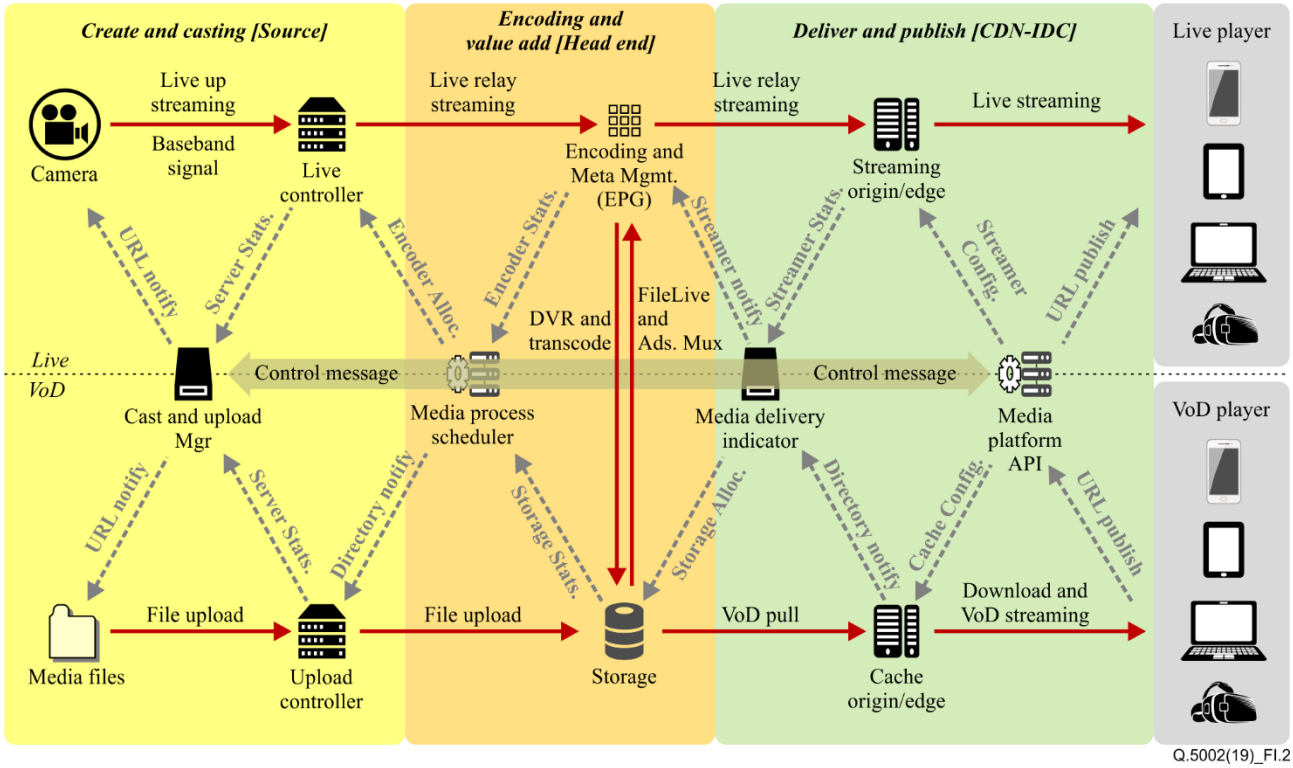

Figure I.2 – Current signalling entities for media services

Future media platform will accommodate various types of devices, which belong to service providers. Moreover, there are a lot of technologies using cloud capability to provide media services to increase user satisfaction. Therefore, the complicated procedures of each cloud computing service provider (e.g., Amazon EC2, Microsoft Azure, Google CE, etc.) need to be integrated.

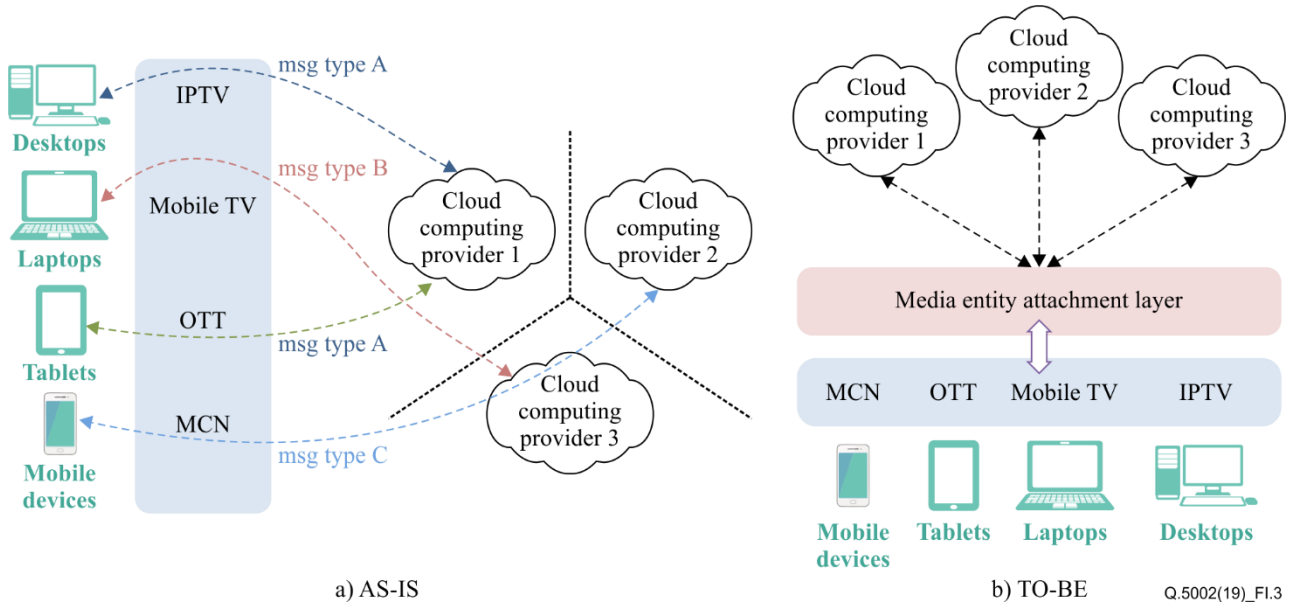

Figure I.3 – Media service architecture using cloud computing capability: (a)AS-IS, (b)TO-BE

Media service providers for different service technologies have always been developed separately and created different verticals. This separate development has some significant drawbacks. Media service providers using cloud capability have to deal with specific signalling flows for all interfaces, which will significantly increase the complexity for the provider to use different cloud computing providers.

Appendix II

Service scenarios using ITU-T Q.5002

(This appendix does not form an integral part of this Recommendation.)

II.1 Service scenario for movie on-demand service

Figure II.1 shows a movie on-demand procedure.

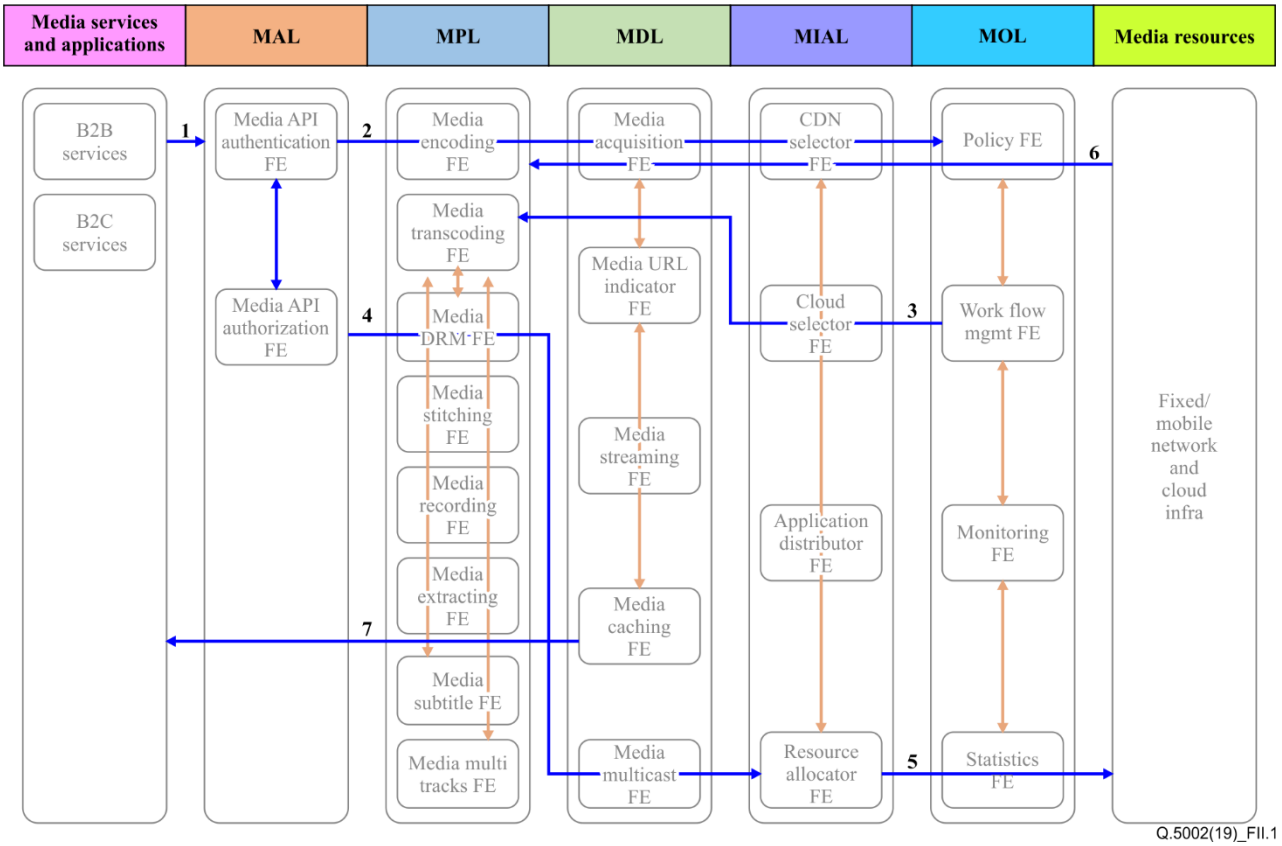

Figure II.1 – Movie on-demand procedure

Movie on-demand service proceeds as follows:

1) An end user requests the movie on-demand service to B2B or B2C service provider. A configuration profile is created for transcoding with information such as scale, resolution, video/audio codec, etc.

2) The requested service is authenticated and authorized in the MAL.

3) Based on the service profile and codec information, the media policy is created and managed for media processing and delivery by the policy FE in the MOL. Then the MOL provides the monitoring FE and the statistics FE to monitor and collect information such as media processing, delivery and service status. The content can be transcoded by the media transcoding FE in the MPL, if needed.

4) When the service request is authorized via the media API authorization FE, the media resource management request message is sent by the media API authorization FE to the resource allocator FE to request aggregate resource allocation based on the service profile.

5) The resource allocation request is triggered by the resource allocator FE when the MIAL receives the media resource management request from the resource allocator FE. Dedicated resources are allocated to Fixed/mobile network or Cloud infra.

6) The content source is delivered by using Web or FTP to a predetermined location in the storage and the location information of the content is registered to the database in the MDL.

7) Finally, the stored content in cache servers delivers to the end user through the media caching FE. For publishing, URLs to download or stream the content over HTTP live streaming (HLS), dynamic adaptive streaming over HTTP (DASH) and HTTP are provided.

II.2 Service scenario for live streaming and recording service

Figure II.2 shows live streaming and recording service procedure.

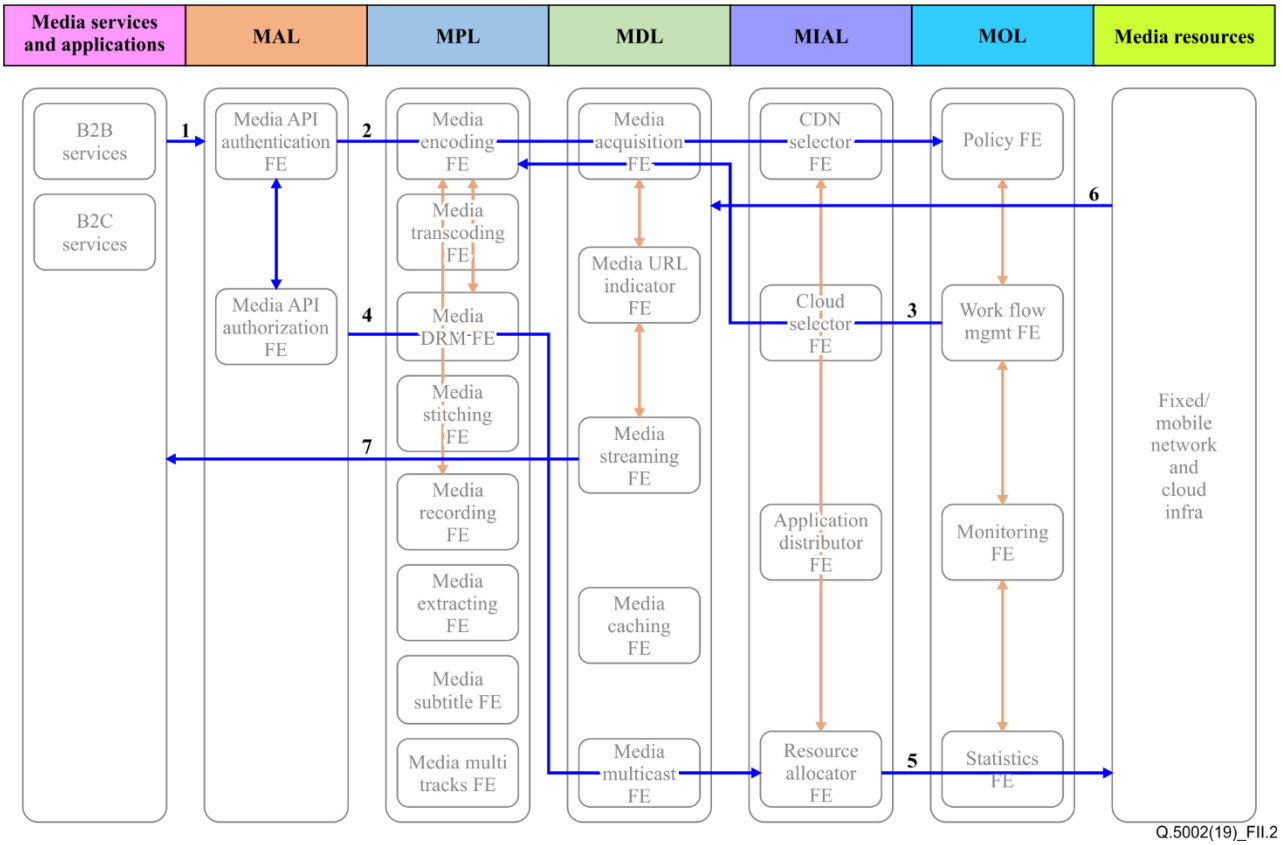

Figure II.2 – Live streaming and recording service procedure

Live streaming and recording service proceeds as follows:

1) An end user requests the live streaming and recording service to B2B or B2C service provider. A configuration profile is created for the live stream encoding with information such as scale, resolution, video/audio codec, etc.

2) The requested service is authenticated and authorized in the MAL. For recording, the configuration profile is installed with information such as source stream URL and file name.

3) Based on the service profile and codec information for the live streaming and recording service, the media policy is created and managed for media processing and delivery by the policy FE in the MOL. Then the MOL provides the monitoring FE and the statistics FE to monitor and collect information such as media encoding process, delivery and service status. The media for the live streaming and recording service can be encoded by the media encoding FE in the MPL, if needed.

4) When the live streaming and recording service request is authorized via the media API authorization FE, the media resource management request message is sent by the media

API authorization FE to the resource allocator FE to request aggregate resource allocation based on the service profile. For publishing, URLs to download or stream the content over HLS, DASH and HTTP are provided.

5) The resource allocation request is triggered by the resource allocator FE when the MIAL receives the media resource management request from the resource allocator FE. Dedicated resources are allocated to Fixed/mobile network or Cloud infra.

6) The media for live streaming and recording service is delivered to a predetermined location in the storage and the location information of the content is registered to the database in the MDL.

7) Finally, the media for live streaming and recording service delivers to the end user through the media streaming FE.

II.3 Service scenario for scheduled live streaming service

Figure II.3 shows scheduled live streaming service procedure.

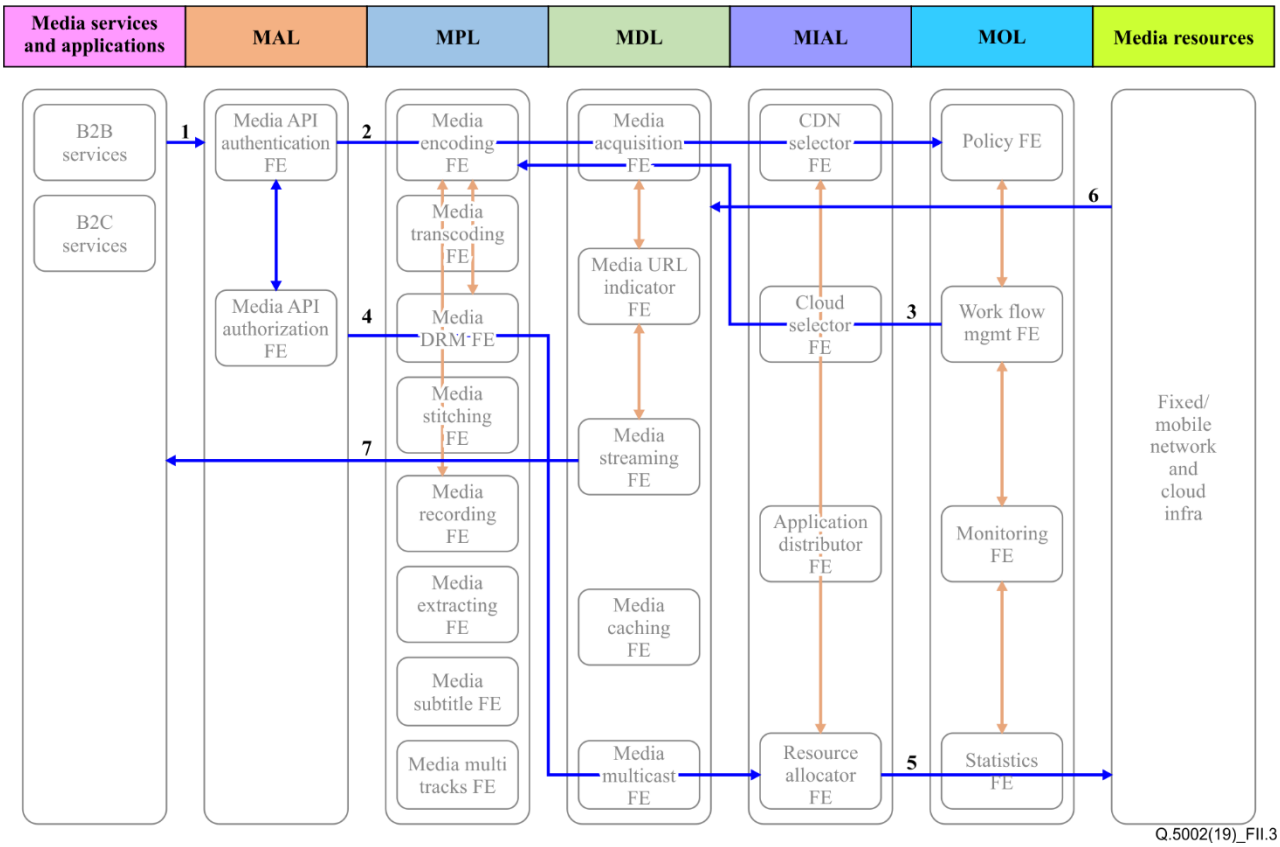

Figure II.3 – Scheduled live streaming service procedure

Scheduled live streaming service proceeds as follows:

1) An end user requests the scheduled live streaming service to B2B or B2C service provider. A configuration profile is created for the live stream encoding with information such as scale, resolution, video/audio codec, etc.

2) The requested service is authenticated and authorized in the MAL. In this procedure, input stream URLs are verified.

3) Based on the service profile and codec information for the scheduled live streaming service, the media policy is created and managed for media processing and scheduled delivery by the policy FE in the MOL. Then the MOL provides the monitoring FE and the statistics FE

to monitor and collect information such as media encoding process, delivery and service status. The media for the scheduled live streaming service can be encoded by the media encoding FE in the MPL, if needed. For the scheduled live streaming service, broadcasting programming such as non-broadcasting programming setup, VoD profile setup and callback URL is set up finally.

4) When the scheduled live streaming service request is authorized via the media API authorization FE, the media resource management request message is sent by the media API authorization FE to the resource allocator FE to request aggregate resource allocation based on the service profile.

5) The resource allocation request is triggered by the resource allocator FE when the MIAL receives the media resource management request from the resource allocator FE. Dedicated resources are allocated to fixed/mobile network or cloud infra.

6) The scheduled live streaming service is delivered to a predetermined location in the storage and the location information of the content is registered to the database in the MDL. For publishing, URLs to download or stream the content over HLS, DASH and HTTP are provided.

7) Finally, the scheduled live streaming service delivers to the end user through the media streaming FE.

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[b-ITU-T X.1603] Recommendation ITU-T X.1603 (2018), *Data security requirements for the monitoring service of cloud computing.*

[b-ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[b-ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service*.

[b-ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management.*

[b-Media Traffic Ratio] *Journal of Information and Telecommunications Vol.35 No.3, KICS (2018, SKT), Next Generation Media Technologies and Architecture.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020