International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.627.1

(03/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband, triple-play and advanced multimedia services – Advanced multimedia services and applications

Protocols for mobile visual surveillance

Recommendation ITU-T H.627.1

ITU-T

International Telecommunication Union

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	**H.620–H.629**
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

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

Recommendation ITU-T H.627.1

Protocols for mobile visual surveillance

Summary

Recommendation ITU-T H.627.1 describes the detailed specification of reference points, message flows control methods and overall protocols of a mobile visual surveillance system based on the requirements described in Recommendation ITU-T F.743 and functional architecture described in Recommendation ITU-T H.626.1.

This Recommendation focuses on the protocols of a visual surveillance system with mobile units and the services related to mobile units, such as a mobile customer unit accessing real-time video stream from a visual surveillance system. This Recommendation defines reference points, message syntax and semantics and relevant protocols.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.627.1	2017-03-01	16	11.1002/1000/13191

Keywords

Message flows, mobile visual surveillance, protocols, reference points.

* 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

Recommendation ITU-T H.627.1

Protocols for mobile visual surveillance

1 Scope

This Recommendation focuses on the protocols of a visual surveillance system with mobile units and the services related to mobile units, such as a mobile customer unit accessing real-time video stream from a visual surveillance system.

This Recommendation defines the reference points and focuses on the protocols for a mobile visual surveillance system, based on the architecture defined in [ITU-T H.626.1].

Furthermore, this Recommendation utilizes and extends some existing protocols such as session initiation protocol (SIP), real-time transport protocol (RTP), real-time streaming protocol (RTSP) and hypertext transfer protocol (HTTP) and also defines the message format and text.

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.

[ITU-T F.743] Recommendation ITU-T F.743 (2009), *Requirements and service description for visual surveillance*.

[ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance*.

[ITU-T H.626.1] Recommendation ITU-TH.626.1 (2013), Architecture for mobile visual surveillance.

[ITU-T H.627] Recommendation ITU-T H.627 (2012), *Signalling and protocols for visual surveillance*.

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*. https://datatracker.ietf.org/doc/rfc3261/

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*. https://datatracker.ietf.org/doc/rfc3550/

[IETF RFC 7231] IETF RFC 7231 (2014), *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. https://datatracker.ietf.org/doc/rfc7231/

[IETF RFC 7826] IETF RFC 7826 (2016), *Real-Time Streaming Protocol Version 2.0*. https://datatracker.ietf.org/doc/rfc7826/

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 customer [b-ITU-T M.60]: A customer is an entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.3 customer unit [ITU-T H.626]: A device located at the customer part of a visual surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.4 functional architecture [b-ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus they define the distribution of functions.

NOTE – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

3.1.5 interface [b-ITU-T Y.101]: A shared boundary between two functional units.

3.1.6 media [b-ITU-T Y.101]: Plural of medium.

3.1.7 medium [b-ITU-T Y.101]: Specific physical support for transmission or storage of information. Type of presentation of information (i.e., video, audio, text, etc.).

3.1.8 mobile customer unit (M_CU) [ITU-T H.626.1]: Mobile client software installed in customers' mobile devices. The M_CU is used to initiate the service and provide customers with video viewing.

3.1.9 mobile service portal (MSP) [ITU-T H.626.1]: A series of devices and subsystems located at the central part of a mobile visual surveillance system. The MSP is the business application platform of the mobile visual surveillance system. Its main functions include a unified access entrance to the business entrance of user authentication and the display list of users' monitoring permissions. The MSP can carry out user authentication, query the list of monitoring permissions, synchronize user account information, and assist service management through the exchange of information with the centre management unit (CMU).

3.1.10 reference point [b-ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

3.1.11 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.12 packet-switched streaming service (PSS) [ITU-T H.626.1]: A device located at the central part of a mobile visual surveillance system. The PSS is the stream media server and processes media stream distribution between the M_CU and the VAU. The main functions of PSS include responding to the service request message sent by M_CU, getting the real-time media stream from VAU and distributing the stream to multiple M_CUs.

3.1.13 premises unit [ITU-T H.626]: A device located at the remote part of a visual surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.14 video access unit (VAU) [ITU-T H.626.1]: A device located at the central part of a mobile visual surveillance system. The VAU is used to implement communication between the mobile customer unit (M_CU) and the units defined in [ITU-T H.626]. The VAU's main functions include: requesting the CMU for scheduling information to be used to establish the media session between the media distribution unit (MDU) and the packet-switched streaming service (PSS), processing requests from the agent mobile customer unit for control of pan/tilt/zoom (PTZ) and distributing and transcoding multimedia data.

3.1.15 visual surveillance [ITU-T H.626]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signal, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CDMA Code Division Multi Access

CMU Centre Management Unit

CU Customer Unit

GW Gateway

HTTP HyperText Transfer Protocol

ID Identification

IP Internet Protocol

IPC IP Camera

M_CU Mobile Customer Unit

MDN Mobile Directory Number

MDU Media Distribution Unit

MIB Management Information Base

MSP Mobile Service Portal

NGN Next Generation Network

NVR Network Video Recorder

PSS Packet-switched streaming service

PTZ Pan/Tilt/Zoom

PU Premises Unit

PUID Premises Unit Identifier

R/W Read/Write

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

RTSP Real-time Streaming Protocol

SCU Service Control Unit

SIP Session Initiation Protocol

SOAP Simple Object Access Protocol

TCP Transmission Control Protocol

UDP User Datagram Protocol

URL Uniform Resource Locator

UTF-8 8-bit Unicode Transformation Format

VAU Video Access Unit

VS Visual Surveillance

WAP Wireless Application Protocol

XML Extensible Markup Language

5 Conventions

In this Recommendation, "String" is a data type used to describe a sequence of characters in UTF-8 format. "Integer" is a datum of integral data type that represents an 8-bit subset of mathematical integers.

6 Message syntax and semantics

[ITU-T H. 626.1] describes the overall architectural framework of mobile visual surveillance as shown in Figure 6-1 and it also introduces reference points of the architecture. This Recommendation gives a more detailed description of these reference points.

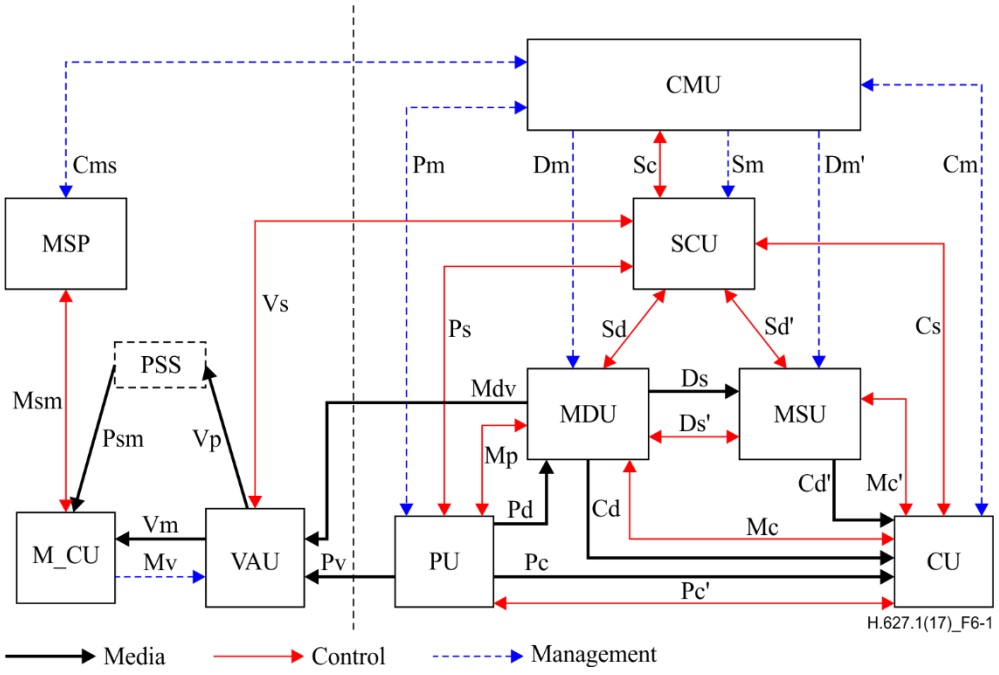

Figure 6-1 – Functional architecture framework of mobile visual surveillance

The interfaces and protocols involved in mobile video surveillance are listed as follows:

1) Reference point Cms: CMU-MSP, uses the Web service interface protocol (SOAP/HTTP)
2) Reference point Msm: MSP-M_CU, uses the HTTP protocol
3) Reference point Mv: M_CU-VAU, uses the user datagram protocol (UDP) communication protocol
4) Reference point Vm: VAU-M_CU, uses the HTTP/RTSP, RTP/RTCP protocol
5) Reference point Psm: PSS-M_CU, uses the HTTP/RTSP, RTP/RTCP protocol
6) Reference point Vs: VAU-SCU, uses the HTTP protocol
7) Reference point Mdv: MDU-VAU, uses the RTP/RTCP protocol
8) Reference point Pv: PU-VAU, uses the RTP/RTCP protocol

9) Reference point Vp: VAU-PSS, uses the RTSP protocol.

6.1 Reference point Cms: CMU-MSP

6.1.1 Interface functions

Reference point Cms is between the centre management unit (CMU) and the mobile service portal (MSP). This interface is used for querying the attributes of the surveillance points when the users log in and to query the information of all surveillance points available for mobile surveillance service:

– User authentication and surveillance point query: When a user logs into the mobile service portal (MSP) using M_CU, the MSP gets the User ID and password of the current user (if the user chooses the universal sign-in way, the MSP needs to translate the mobile directory number (MDN) number into the corresponding User ID and password locally), then the MSP authenticates the user to the centre management unit (CMU) of the video surveillance platform via the User ID and password. If authentication fails, the failed message is returned. If it succeeds, the CMU will query the surveillance point information according to the current User ID, the CMU returns the corresponding surveillance point and parameter list under the User ID in the MSP.

– Query the enterprise surveillance points attribution: When an enterprise user logs into the Enterprise Self-Service system through the MSP, the MSP gets the relevant information of the current surveillance point list that the enterprise has activated on the CMU video surveillance platform through the enterprise account.

– RTSP media stream entrance query: When a user queries certain kinds of media streaming from a surveillance point, the CMU returns the RTSP access address that the user gets through internal query scheduling on the platform.

NOTE – Access to the media requires the access token.

An authorized user requests resources according to the original interface specification, called "reqUserChannelInfo".

6.1.2 Interface protocols

This interface uses IP protocol and the Web service interface protocol (SOAP/HTTP).

6.1.3 Message format

1) The enterprise attribute information query

The MSP queries the enterprise attribute information according to the corporate identity (customerID) with the parameters indicated in Table 6.1-1. The parameters returned are found in Table 6.1-2.

Table 6.1-1 – Interface: MSP→CMU

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
CustomerId	Enterprise ID	String	Telecom administrator manually input when the MSP service opened (18 bits). The first six bits of customerID refer to the domain ID (platform domain).

Table 6.1-2 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
CustomerName	Customer names	String	
CustomerType	Customer type	Integer	Only : Enterprise:1
Address	Customer address	String	
PhoneNumber	Customer phone number	String	
Fax	Customer fax number	String	
ZipCode	Customer zip code	String	
Email	Customer E-mail	String	
TransactPerson	The operator	String	
AdminAccount	Video surveillance admin account	String	
ResultCode	Return code	Integer	0 if enterprise ID does not exist 1 for access success
NOTE – The user uses "adminAccount prefix" to login to the MSP Enterprise Self-Service page, the user ID and user account are in the same format.			

2) Search enterprise information list

The MSP queries the enterprise attribute information according to the corporate identity (customer ID) or customer name with the parameters listed in Table 6.1-3. The returned parameters are listed in Table 6.1-4.

Table 6.1-3 – Interface: MSP→CMU

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
searchCID	Enterprise ID	String	Telecom administrator manually inputs when the MSP service opened (18). The first six bits of customerID refer to the domain ID (Platform domain).
searchCN	Enterprise name	String	Company name

Table 6.1-4 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
CustomerName	Customer names	String	
CustomerType	Customer type	Integer	Only : Enterprise:1
Address	Customer address	String	
PhoneNumber	Customer phone number	String	
Fax	Customer fax number	String	

Table 6.1-4 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
ZipCode	Customer zip code	String	
Email	Customer E-mail	String	
TransactPerson	The operator	String	
AdminAccount	Video surveillance admin account	String	
NOTE – User uses "adminAccount prefix" to login to the MSP Enterprise Self Service page, the user ID and user account use the same format.			

3) Accept MSP user authentication

The CMU accepts the MSP user authentication, including the user's login through a mobile phone and the enterprise administrator with the parameters listed in Table 6.1-5. The returned parameters are listed in Table 6.1-6.

Table 6.1-5 – Interface: MSP→CMU

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain", which is the account is the MSP user account or the enterprise administrator accounts which has been previously processed NOTE – When the corresponding video surveillance platform does not have the customer domain, only need to fill in the user name.
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
AccountType	User account type	Integer	0 for a user 1 for enterprise administrator

Table 6.1-6 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
Authorization	Certification results	Integer	0 for failure, 1 for success
The following list of fields			
CategoryID	Catalogue number	String	
CategoryName	Catalogue name	String	
PID	The parent ID	String	PID is the parent directory of the CategoryID. The value is null when CategoryID is the root directory

4) User account query by the customer

The enterprise administrator queries for the list of all user accounts opened by the enterprise with the parameters listed in Table 6.1-7. The returned parameters are listed in Table 6.1-8.

Table 6.1-7 – Interface: MSP→CMU

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
CustomerId	Enterprise ID	String	The first six bits of customerID refer to the domain ID

Table 6.1-8 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
ResultCode	Return code	Integer	0 if enterprise ID does not exist 1 for success
Account	User account	String	"username@userdomain" NOTE – When the corresponding video surveillance platform does not contain the customer domain, only the user name is used.

5) Attribution query of the common surveillance point user

A query for the authorized surveillance list under the specific user account is sent using the parameters listed in Table 6.1-9. The returned parameters are listed in Table 6.1-10.

Table 6.1-9 – Interface: MSP→CMU

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain", which is the MSP user account which has previously been processed NOTE – When the corresponding video surveillance platform does not contain the customer domain, only the user name is used.
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
CategoryID	Catalogue number	String	Catalogue numbers is a null value representing the query root directory

Table 6.1-10 – Interface: CMU→MSP

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
PuId-ChannelNo	PU Channel Number	String	
PuName	PUname	String	
PtzFlag	Control authority flag	Integer	0: no authorization; 1: authorization
PlaybackFlag	Playback authority flag	Integer	0: no authorization; 1: authorization
Online	Online flag	Integer	0: offline; 1: online
ResultCode	Return code	Integer	0: no user account; 1: success

6) Query the VAU and PTZ addresses

A query for the RTSP address of video access unit (VAU) entrance and pan/tilt/zoom (PTZ) entrance is sent using the parameters listed in Table 6.1-11. The returned parameters returned from the video surveillance system to MSP are listed in Table 6.1-12. In addition to the VideoPlayUrl VAU/PSS address, the reply also contains the fields in Table 6.1-13.

Table 6.1-11 – Interface: reqVauUrlRequest

MSP-CMU interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain" NOTE – When the corresponding video surveillance platform does not contain the customer domain, only the user name is used.
M_cuIp (Optional)	M_CU's IP address	String	Because VAU can span multiple network deployment. This parameter is provided to CMUand used to determine the return VAU which segment address. By default M_CU fill in 0.0.0.0, CMU returns VAU foreign service public address.
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
PuId-ChannelNo	Surveillance point unique identifier	String	
PlayMethod	Play type	Integer	0: Real-time video 1: Video recording

Table 6.1-12 – Interface: reqVauAddResponse

CMU-MSP interface parameters			
Parameter	**Parameter name**	**Data type**	**Notes**
CMUPtzUrl	CMU PTZ URL address	String	Return CMU PTZ URL address
VideoPlayUrl	Direct access entrance	String	Return Direct access entrance URL address (PSS or VAU address)

Table 6.1-13 – VideoPlayUrl parameter fields

Parameter	Parameter name	Data type	Notes
Account	User account	String	"username@userdomain" NOTE – When the corresponding video surveillance platform does not contain the customer domain, only the user name is used.
PuId-ChannelNo	Unique identifier of the surveillance point	String	
PlayMethod	Play type	Integer	0: real-time video (fixed as 0 at present)
ExpireTime	Requesting the link failure time	String	20120406155530 Year-month-day-hour-min-sec
HashToken	MD5 abstract	String	Calculated as the MD5 hash of a string containing user name, password hash, PuID-ChannelNo and ExpireTime, in the form: HEX(MD5(Account=*xx*&Password=*HEX(MD5(password))*&PuID-ChannelNo=*nn*&ExpireTime=*tt*)) NOTE – Step 1: calculate the MD5 hash of the password and use the hexadecimal uppercase string – HEX(MD5(*password*)); Step 2: Use the result of step 1 to compose the string "Account=*xx*&Password=*HEX(MD5(password))*& PuID-ChannelNo=*nn*&ExpireTime=*tt*" (without quotes), then calculate its MD5 hash and use its hexadecimal uppercase string.

Hash Token requirements:

– If the HashToken parameter value in VideoPlayUrl was artificially modified, VAU should deny authentication;

– If the VideoPlayUrl video link request time exceeds the ExpireTime value, the link is invalid;

However, video streaming could continue to play in the established RTSP media channels, not subject to the ExpireTime time limit.

6.2 Reference point Msm: MSP-M_CU

6.2.1 Interface functions

Reference point Psm is between the MSP and the M_CU. The M_CU and MSP interface uses Web service interface protocol (SOAP/HTTP), mainly to complete the following functions:

– Send the service request; realize video surveillance business connecting and authentication through MSP;

– Get control point play entrance;

– Check version.

6.2.2 Interface protocols

The M_CU and MSP interface uses the IP protocol and the Web service interface protocol (SOAP/HTTP).

6.2.3 Message format

Tables 6.2-1 to 6.2-7 describe the message format for M_CU authentication certification and packet access, MSP-M_CU, surveillance points list query and response, video surveillance point play entrance query and response and duration statistics for mobile surveillance video.

Table 6.2-1 – Parameters for M_CU authentication certification and packet access

M_CU→MSP			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain"
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
LoginType	Login type	Integer	0: Account-password login 1: Local login
Version	M_CU version	String	For example: V1.05.004, larger version needs to be consistent with MSP. If the version of MSP>M_CU that M_CU L / class; if M_CU>MSP version, then prompts the current version of M_CU is too high, please use the low version.

Table 6.2-2 – Return information from MSP to an M_CU authentication certification and packet access request

MSP→M_CU			
Parameter	**Parameter name**	**Data type**	**Notes**
Result	Certification results	Integer	0: Success 1: User name does not exist 2: Wrong password 3: M_CU version too new 4: M_CU version too old
The following list			
CategoryID	CategoryID	String	
CategoryName	CategoryName	String	
PID	The parent ID	String	PID is the parent directory of the CategoryID. The value is null when CategoryID is the root directory.

Table 6.2-3 – Parameters for a surveillance points list query

M_CU→MSP			
Parameter	**Parameter name**	**Data type**	**Notes**
M_cuIp	M_CU's IP address	String	Because VAU can span multiple network deployments. This parameter is provided to CMU and used to determine the return VAU which segment address. By default, M_CU fill in 0.0.0.0, CMU returns VAU foreign service public address.
Account	User account	String	"username@userdomain"
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
CategoryID	Catalogue number	String	Catalogue numbers is a null value representing the query root directory

Table 6.2-4 – Return information for a surveillance point query

MSP→M_CU			
Parameter	**Parameter name**	**Data type**	**Notes**
PuId-ChannelNo	PU number and Channel Number	String	Corresponds to the PU number and channel number.
PuProperty	PU ability of PTZ control	Integer	It is the PU ability of PTZ control. If no control ability, default is 0
PuName	Surveillance point name	String	For prompting the user to PU the specific significance in M_CU
Online	Online flag	Integer	0 for offline; 1 for online

Table 6.2-5 –Entrance query parameters for a video surveillance point play

M_CU→MSP			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain"
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
PuId-ChannelNo	PU number and Channel Number	String	

Table 6.2-6 – Return information to a video surveillance point play entrance query

MSP→M_CU			
Parameter	**Parameter name**	**Data type**	**Notes**
CMUPtzUrl	CMU PTZ URL address	String	Return CMU PTZ URL address
VideoPlayUrl	Direct access entrance	String	Return Direct access entrance URL address (PSS or VAU address)

Table 6.2-7 – Duration statistics for mobile surveillance video data flow

M_CU→MSP			
Parameter	**Parameter name**	**Data type**	**Notes**
Account	User account	String	"username@userdomain"
Password	User password	String	Mandatory, 32 uppercase characters for MD5 coding of password, such as: "96E79218965EB72C92A549DD5A330112"
BRun	Start / end flag	Integer	0: Start 1: Process (heartbeat) 2: Quit
NStreamBit	Video data flow	Integer	The unit is Kbyte
NStreamTime	Video data time	Integer	The unit is second

6.3 Reference point Psm: M_CU- PSS

6.3.1 Interface functions

Reference point Psm is between the M_CU and the PSS.

The interface is used to transmit data through HTTP and RTSP to:

– Send service request, carrying service and user information

– Establish connection and transmit real-time media stream and real-time video

– Play video according to operations such as pause, continue, forward and other orders.

6.3.2 Interface protocols

This interface is actually between the terminal and the streaming server. It follows the TCP / IP, RTP / RTSP / RTCP protocol, as shown in Figure 6-2.

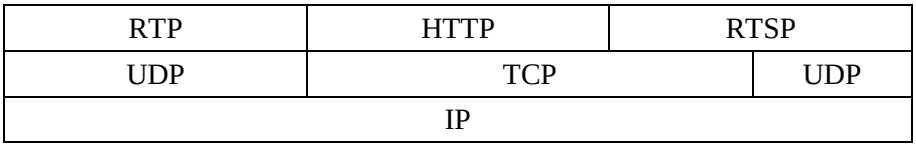

Figure 6-2 – Interface protocol

6.3.3 Message format

6.3.3.1 HTTP interface

This interface is realized through the parameters carried by HTTP URL. When a user clicks on the URL generated by the MSP, the parameters listed in Table 6.3-1 are acquired and transferred to PSS without processing.

See [IETF RFC 7231] for HTTP message.

Table 6.3-1 – HTTP parameters from M_CU to PSS

M_CU→PSS			
Parameter	**Parameter name**	**Data type**	**Value**
UserId	User ID	String	
PuID-ChannelNo	Unique identification of surveillance point	String	
PuProperty	Whether PU has PTZ function	Integer	NOTE – Default value is 0 if PU does not have PTZ function
VAUADD	VAU address and PTZ control port	String	Format: xxx.xxx.xxx.xxx:xxx(ip: port) NOTE – Default value is 0 if PU does not have PTZ function. This parameter is validated only in real-time mode.

When a user requests PSS service, the HTTP request format is as follows:

```
http://pssIp:port/service?userid=xx&PuID-ChannelNo=xx&puproperty=xx&vauadd=xx
```

PSS responds to the M_CU request, and sends the dynamically generated RTSP URL to the end user automatically through html page jumping, the address is as follows:

```
<head>
     <meta content="refresh" url="0,rtsp://xxxxxxxxxxxxxxxxx"/>
</head>
```

6.3.3.2 RTSP interface

The RTSP message is for establishment and control of streaming transferring dialog, see [IETF RFC 7826] for details. The RTSP request sent by the M_CU to the PSS should carry the parameters listed in Table 6.3-2.

Table 6.3-2 – RTSP parameters from M_CU to PSS

M_CU→PSS			
Parameter	**Parameter name**	**Data type**	**Value**
UserId	User ID	String	
PuID-ChannelNo	Unique identification of surveillance point	String	
PlayMethod	Media type	Integer	0: Real-time 1: Video record
StartTime	Start time of recording	String	Format: 20120406155530 Year-month-day-hour-min-sec
PuProperty	Whether PU has PTZ function	Integer	NOTE – Default value is 0 if PU does not have PTZ function.
VAUADD	VAU address and PTZ control port	String	Format: xxx.xxx.xxx.xxx:xxx(ip: port) NOTE – Default value is 0 if PU does not have PTZ function. This parameter is validate only in realtime mode.

Table 6.3-2 – RTSP parameters from M_CU to PSS

M_CU→PSS			
Parameter	**Parameter name**	**Data type**	**Value**
hashtoken	For billing authentication request	String	Used by manufactories for anti-stealing-link, not be processed by M_CU

Parameters are transmitted through:

```
RTSP://localhost:port/service?UserID= XXX & PID= XXX……
```

The server of the RTSP extracts parameters while responding to the request and processes them according to the service logic.

M_CU send RTSP requests through VideoPlayUrl CMS querying by MSP.

This is a sample URL:

```
rtsp://VideoPlayUrl/service?Account=xx&PUID-ChannelNo=xx &
ExpireTime=xx&HashToken=xx
```

6.4 Reference point Vm: M_CU- VAU

6.4.1 Interface function

Reference point Vm is between M_CU and the video access unit (VAU).

It is used to transmit the real-time video through RTSP.

6.4.2 Interface protocols

This interface uses RTSP protocol, the M_CU works as the RTSP client, the VAU works as the RTSP server which can be configured freely and the default port is 554. The RTSP message format and parameters are indicated in Tables 6.4-1 and 6.4-2.

Table 6.4-1 – Common parameters from M_CU to VAU

M_CU→VAU			
Parameter	**Parameter name**	**Data type**	**Value**
PlayMethod	Media type	String	0: Real-time video 1: Video recording

Table 6.4-2 – Real-time mode parameters from M_CU to VAU

M_CU→VAU			
Parameter	**Parameter name**	**Data type**	**Value**
PuID-ChannelNo	Channel identification, the PUID and channel number in VS system	String	

The format of real-time video viewing RTSP URL is as follows:

```
rtsp://vauaddress:port/service?PuID-ChannelNo=XXXXXXXXXXXX-X PlayMethod=0,
```

For instance:

```
rtsp://172.24.202.190/service?PuID-ChannelNo=320101000200000001-1&&PlayMethod=0,
```

which refers to accessing the first channel of PU No. 320101000200000001's real-time video stream.

6.4.3 Message format

The M_CU works as the client and the VAU works as the server, the messages are as follows:

Minimum requirements of client and server basic playback can be found in [IETF RFC 7826].

DESCRIBE message

1) The M_CU sends DESCRIBE message.
2) The VAU returns 200 OK with correct message body to the M_CU, establishing the session. The message body includes the default video CODEC of the transferred video stream and related profile-level-id, frame rate, frame size and so on. VAU configures the default value.

SETUP message

1) The M_CU sends SETUP message, describing the interface which receives the media streaming.
2) The VAU returns 200 OK to the M_CU, describing the interface which sends the media streaming.

PLAY message

1) The M_CU sends PLAY message.
2) The VAU starts to play real-time video or video record.
3) The VAU returns 200 OK to M_CU.
4) The VAU starts to send media stream to the M_CU.

PAUSE message

1) The M_CU sends the correct PAUSE message.
2) The VAU pauses the real-time video or video record playing.
3) The VAU returns 200 OK to M_CU.
4) The VAU stops sending media stream.

TEARDOWN message

1) The M_CU sends TEARDOWN message.
2) The VAU stops the real-time video or video record playing.
3) The VAU returns 200 OK to the M_CU.
4) The VAU stops sending media stream.
5) The VAU RTSP SOCK stops.

OPTIONS message

1) The VAU sends OPTIONS message to the M_CU (with Session).
2) The M_CU searches for the target Session.
3) If the target Session exists, the M_CU returns 200 OK. If the target Session does not exist, the M_CU returns 404 error and the VAU disconnects the Session with the CMU and releases the source.

6.5 Reference point Mv: M_CU-VAU

6.5.1 Interface function

Reference point Mv is between M_CU and VAU and it is used to control PTZ when end-users browse real-time video.

6.5.2 Interface protocols

The communication between the M_CU and the VAU is according to UDP protocol. The default communication port is 5060. The package for request and response reserves 200 bytes for via fields in the header field of SIP.

The M_CU sends the PTZ control messages to VAU without 200 OK response or resend. But if within the specified time period M_CU does not send the stop message to VAU, VAU will send PTZ stop message to the platform automatically.

Considering the case where multiple M_CUs visit one PuID-ChannelNo at the same time, M_CU will send the PuID-ChannelNo carried by RTSP request to the VAU. The VAU distinguishes PTZ message target devices according to the PTZ message body.

6.5.2.1 M_CU

The M_CU sends a request and receives a response. When it receives a response, the M_CU must check the XML file.

Message_Type and Sequence_Number. If the parameter is wrong, the response must be discarded.

6.5.2.2 VAU

The VAU should be able to receive a request from any IP address and port and reply to the port from the M_CU request.

6.5.3 Message format

The message format follows the following structure:

```
generic-message = start-line
*message-header
CRLF
[ message-body ]
```

6.5.3.1 start-line

The start-line is either Request-Line or Status-Line, as follows.

SIP request:

```
Request-Line = Method SP Request-URI SP SIP-Version CRLF
```

SIP response:

```
Status-Line = SIP-Version SP Status-Code SP Reason-Phrase CRLF
```

6.5.3.2 message-header

Request for message-header:

```
INFO sip:xxx
Content-Type: application/global_eye_v10+xml
Content-Length: xxx
To: xxx
From: xxx
CSeq: xxx INFO
Call-ID: xxx
```

```
Max-Forwards: xxx
Via: xxx
Contact: xxx
[CrLF]
```

Response to message-header:

```
200 OK sip:xxx
Content-Type: application/global_eye_v10+xml
Content-Length: xxx
To: xxx
From: xxx
CSeq: xxx INFO
Call-ID: xxx
Max-Forwards: xxx
Via: xxx
Contact: xxx
[CrLF]
```

6.5.3.3 Message-body

PTZ control

a) Function: The user platform sends PTZ control messages to another platform.

b) Message:

```
<!—PTZ control -->
<?xml version="1.0" encoding="UTF-8" ?>
<Message Verison="1.0">
<IE_HEADER MessageType="MSG_PTZ_SET_REQ"
  UserID="User name"
  DestID="PuID-ChannelNo"
/>
<IE_PTZ OpId="code"
  Param1=" parameter 1"
  Param2=" parameter 2"
/>
</Message>
```

This message needs no response.

6.5.3.4 List of codes and parameters

The list of codes and parameters for PTZ control messages is given in Table 6.5-1.

Table 6.5-1 – Codes and parameters for PTZ control messages

1: turn up (1..10)	11: RESERVED
2: turn down (1..10)	12: RESERVED
3: turn left (1..10)	13: RESERVED
4: turn right (1..1)	14: RESERVED
5: open iris (1..10)	15: stop
6: close iris (1..10)	20: scan off
7: zoom in (1..10)	21: scan on (1..10)
8: zoom out (1..10)	24: RESERVED
9: focus near (1..10)	25: RESERVED
10: focus far (1..10)	26: RESERVED

6.6 Reference point Vp: VAU-PSS

6.6.1 Interface functions

Reference point Vp is between the VAU and the PSS.

It is used to transfer performance data, alarm data and topological data.

6.6.2 Interface protocols

Interface protocols are HTPP+XML, SOAP or CORBA for different platforms and systems.

6.6.3 Message format

6.6.3.1 VAU interface

The VAU interface is used to control and manage the VAU according to the definition of the management information base (MIB).

The VAU information model is described in Tables 6.6-1, 6.6-2 and 6.6-3. The state management is defined in Table 6.6-3.

Table 6.6-1 – VAU interface

Name	Data type	Read/Write
VAU device ID	String	R/W
Version number	String	R/W
Equipment manufacturer code	String	R/W
Equipment manufacturer name	String	R/W
IP network parameter	String	R/W
Maximum number of video input	Integer	R/W
Maximum number of video output	Integer	R/W
Transcoding type	String	R/W
Platform number	Integer	R/W

Table 6.6-2 – VAU multi-platform data structure

Name	Data type	Read/Write
CMS device ID	String	R/W
IP address	String	R/W
Port	String	R/W

Table 6.6-3 – VAU state management information data structure

Name	Date type	Read/Write
VAU device ID	String	R
CPU usage	String	R
Memory usage	String	R
Current processes number	Integer	R
Current thread number	Integer	R
Registration status	String	R
Current video inputs	Integer	R
Current video outputs	Integer	R
Current transcoding number	Integer	R
VAU heartbeat statue	String	R

6.6.3.2 PSS interface

This is the MIB definition of PSS management, which can be used to control and manage the PSS.

Configuration management is described in Table 6.6-4.

State management is described in Table 6.6-5.

Table 6.6-4 – PSS configuration management data structure

Name	Data type	Read/Write
PSS device ID	String	R/W
Version Number	String	R/W
Equipment manufacturer code	String	R/W
Equipment manufacturer name	String	R/W
Maximum number of video input	Integer	R/W
Maximum number of video output	Integer	R/W

Table 6.6-5 – PSS state management data structure

Name	Data type	Read/Write
PSS device ID	String	R
CPU usage	String	R
Memory usage	String	R
Current processes number	Integer	R
Current thread number	Integer	R
Registration status	String	R
Current video inputs	Integer	R
Current transcoding number	Integer	R
PSS heartbeat statue	String	R

6.7 Reference points Mdv/Pv/Vs:VAU-VS system

Reference points Mdv, Pv, Vs are all between the VAU and the visual surveillance (VS) system which are all internal interfaces, there is no specific definition in this Recommendation.

7 Message flows

In this clause, the message flows of main functions are described, including real-time video/audio acquisition, recording and playback, PTZ control, resource query and service management. The following are illustrative items:

– The SIP message format should comply with the definition in [IETF RFC 3261]

– The RTSP message format should comply with the definition in [IETF RFC 7826]

– The HTTP message format should comply with HTTP1.1 defined in [IETF RFC 7231]

– RTP/RTCP signalling message refers to [IETF RFC 3550].

7.1 Real-time video/audio acquisition

Real-time video/audio acquisition is used to view the real-time surveillance video/audio data by mobile terminals. After the MSP performs authentication and returns the VAU information, the M_CU chooses and requests the VAU for real-time video/audio data.

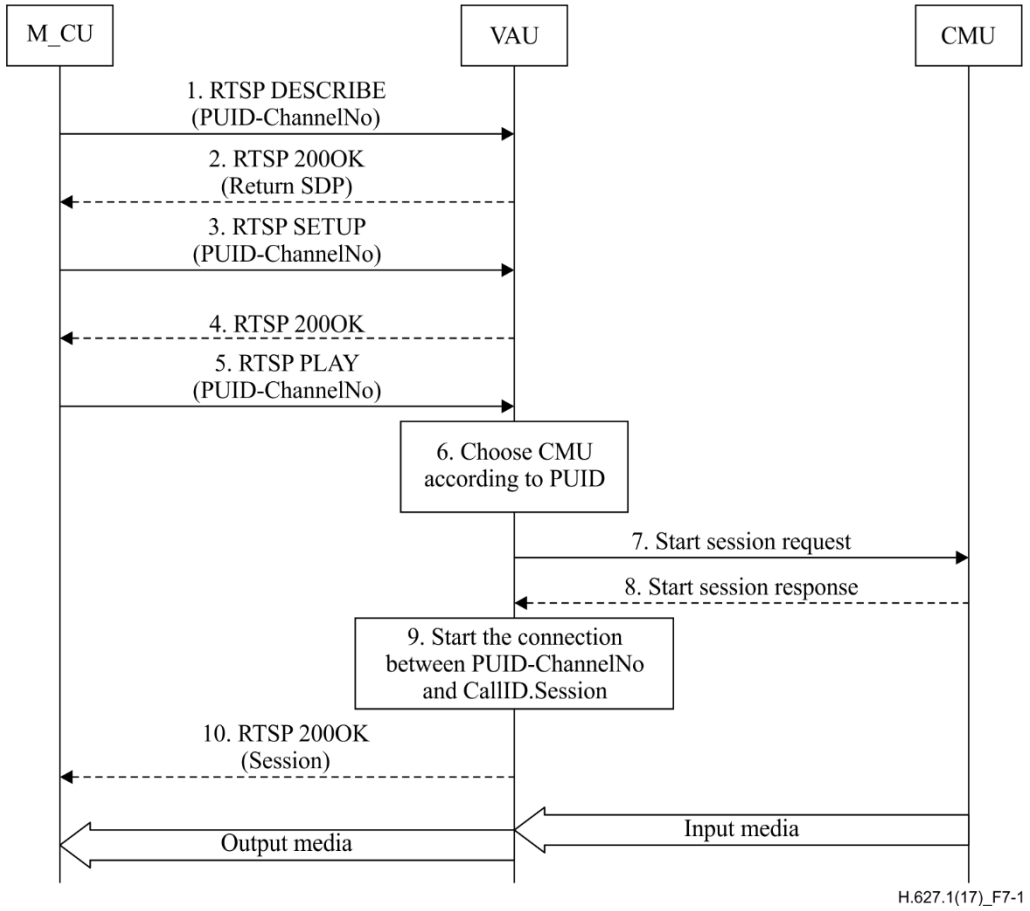

Figure 7-1 – High level procedural flows for real-time media acquisition

The message flows for real-time video/audio acquisition, illustrated in Figure 7-1, are as follows:

1) The M_CU sends RTSP DESCRIBE (PuID-ChannelNo) to the VAU.

2) The VAU returns response message to the M_CU according to parameter configuration.

3) The M_CU sends RTSP SETUP request to the VAU.

4) The VAU distributes a channel and returns RTSP 200OK response message to the M_CU.

5) The M_CU sends RTSP PLAY request to the VAU for real-time video surveillance.

6) The VAU chooses the CMU according to premises unit identifier (PUID).

7) The VAU starts session request to the CMU.

8) The CMU returns session response to the VAU. If the VAU provides video format message body, the CMU chooses a codec that the PU supports and returns the message body to the VAU. If the VAU does not offer message body information, the CMU returns the message body carrying all the capacities that the PU supports to the VAU.

9) The VAU judges the media data format and decides whether to start the transcoding process. The VAU starts the connection between PuID-ChannelNo and CallID and creates a RTSP Session NO.

10) The VAU sends a session control response message to the M_CU.

7.2 Recording and playback

The playback function is used to play audio and video which has been previously recorded and stored.

7.2.1 Playback in platform

When users want to playback the surveillance video using mobile phones, they must log into the MSP by the M_CU. The MSP performs authentication and returns the playback surveillance list.

After the users choose one surveillance point name, the M_CU sends a request for this surveillance video to the VAU and then the VAU returns the media stream to the M_CU to play.

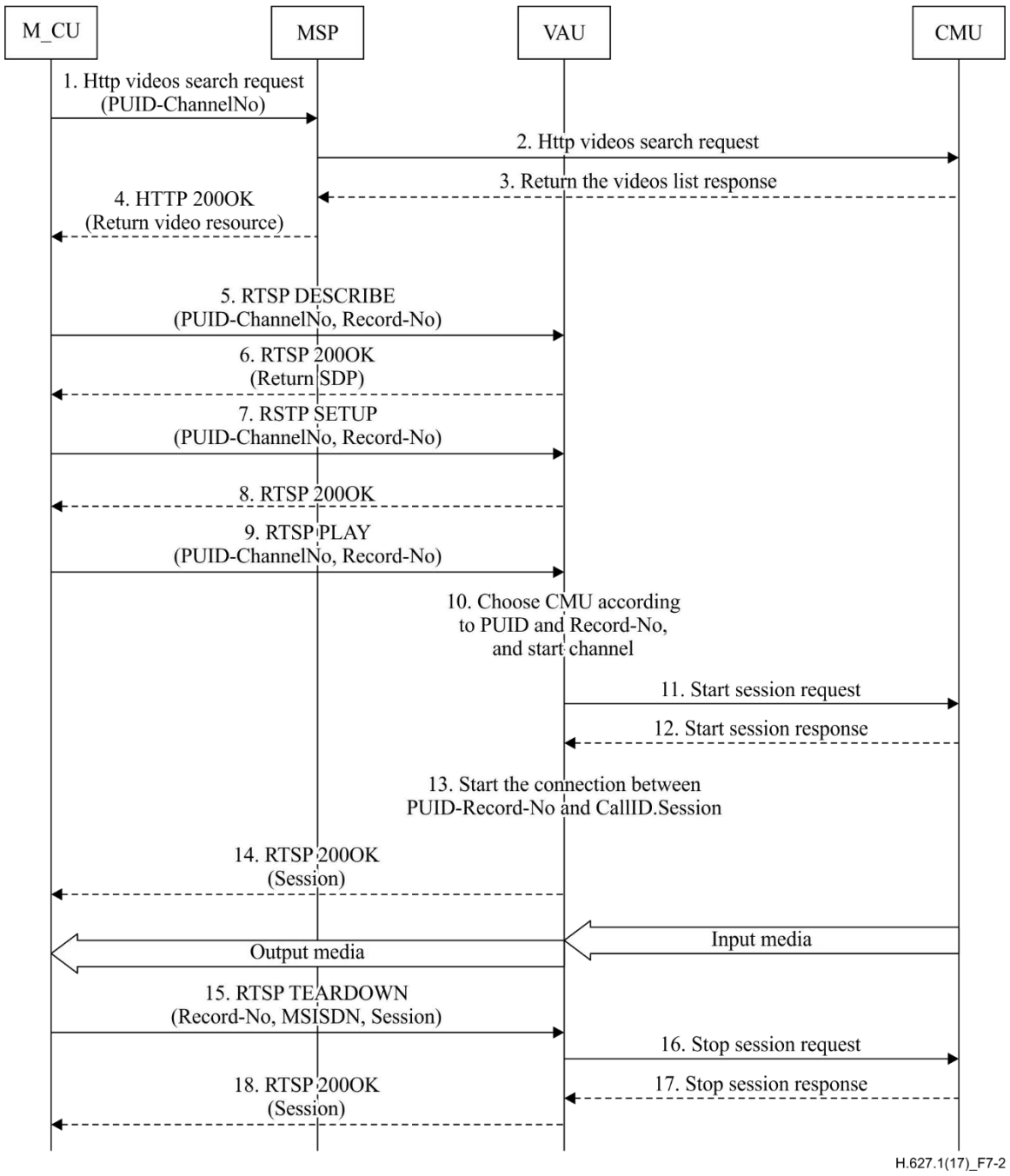

Figure 7-2 – Video playback from the platform procedural flows

The message flows for playback in the platform, illustrated in Figure 7-2, are as follows:

1) The M_CU sends http video search request (PuID-ChannelNo) to the MSP.
2) The MSP sends http video search request (PuID-ChannelNo) to the CMU.
3) The CMU returns the video list information to the MSP.
4) The MSP returns the video list information to the M_CU. Each video is assigned a unique Record-No in the CMU.
5) The M_CU sends RTSP DESCRIBE (PuID-ChannelNo, Record-No) to the VAU.
6) The VAU returns a response message to the M_CU according to the parameter configuration.
7) The M_CU sends RTSP SETUP request to the VAU.

8) The VAU distributes a channel and returns RTSP 200OK response message to the M_CU.

9) The M_CU sends RTSP PLAY request to the VAU for videos record (PuID-ChannelNo, Record-No).

10) The VAU chooses the CMU according to PUID and Record-No.

11) The VAU starts session request to the CMU. The request message carries the message body including the video format which the VAU supports.

12) The CMU returns a session response to the VAU. If the VAU provides a video format message body, the CMU chooses the codec which the PU supports and returns the message body to the VAU. If the VAU does not offer message body information, the CMU returns the message body carrying all capabilities which the PU supports to the VAU.

13) The VAU decides whether to start the transcoding process according to the media data format. The VAU starts the connection between PuID-ChannelNo, RecordNo and CallID, and creates a RTSP Session No.

14) The VAU sends a session response message to the M_CU.

15) The M_CU sends RTSP TEARDOWN to the VAU in order to remove the real-time session.

16) The VAU sends the end request to the CMU to stop the session.

17) The CMU sends the end response to the VAU to stop the session.

18) The VAU sends the end response to the M_CU to stop the session.

7.2.2 Playback in PU

The message flows for playback in the premises unit are illustrated in Figure 7-3.

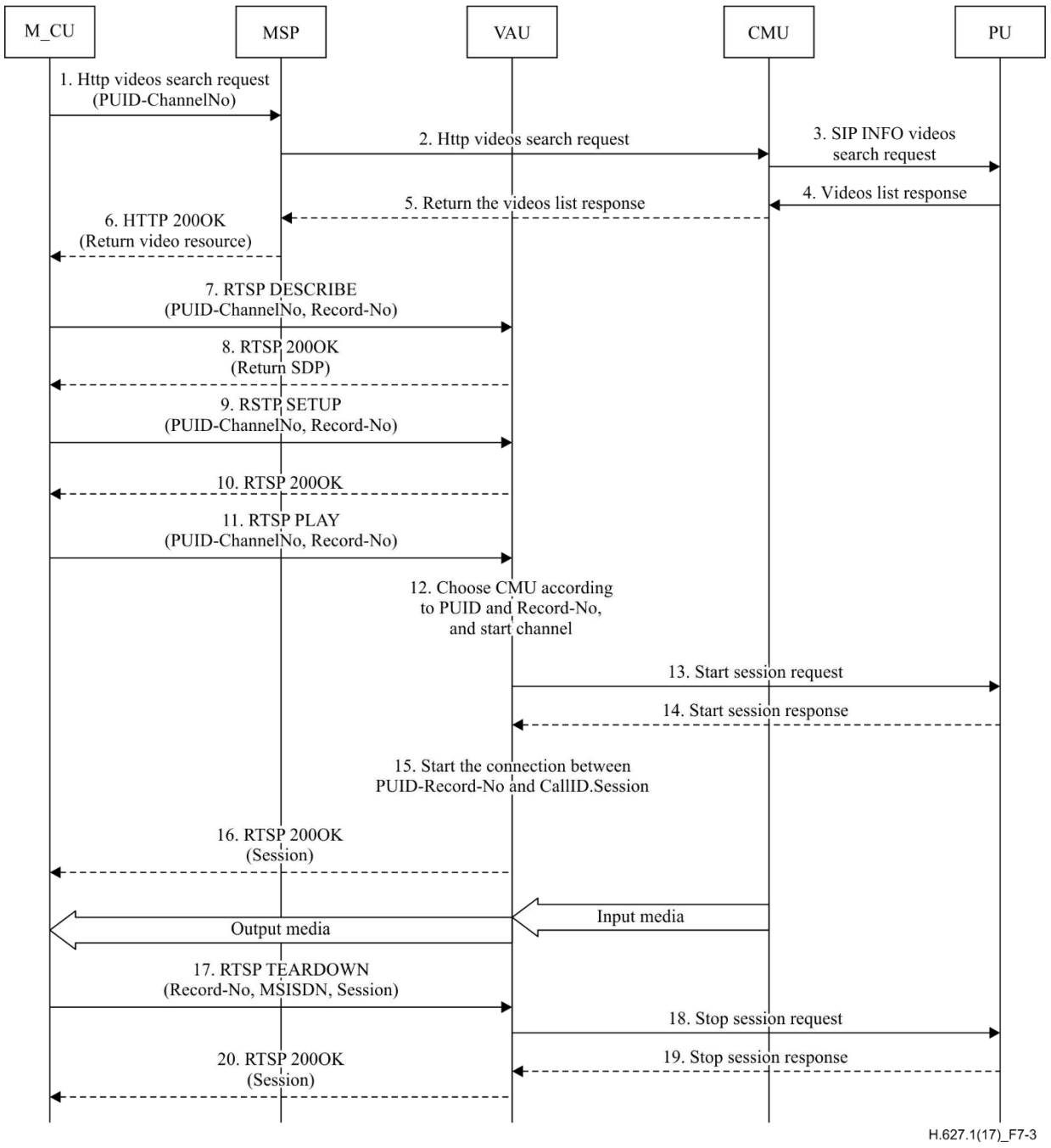

Figure 7-3 – Video playback from the PU procedural flows

The message flows for playback in the PU, illustrated in Figure 7-3, are as follows:

1) The M_CU sends a http video search request (PuID-ChannelNo) to the MSP.
2) The MSP sends a http video search request (PuID-ChannelNo) to the CMU.
3) The CMU sends a SIP(INFO) request to the PU for videos list information (PuID-ChannelNo).
4) The PU returns the video list information to the CMU.
5) The CMU returns video list information to the MSP.
6) The MSP returns the video list information to the M_CU. The CMU distributes the Record-No to the videos
7) The M_CU sends RTSP DESCRIBE (PuID-ChannelNo, Record-No) to the VAU.

8) The VAU returns a response message to the M_CU according to parameter configuration.

9) The M_CU sends a RTSP SETUP request to the VAU.

10) The VAU distributes a channel and returns RTSP 200OK response message to the M_CU.

11) The M_CU sends RTSP PLAY request to the VAU for videos record (PuID-ChannelNo, Record-No).

12) The VAU chooses the CMU according to PUID and Record-No.

13) The VAU starts a session request to the PU. The request message carries message body including the video format which the VAU supports.

14) The PU returns a session response to the VAU. If the VAU provides the video format message body, the CMU chooses the codec which the PU supports and returns the message body to the VAU. If the VAU does not offer message body information, the CMU returns the message body carrying all capabilities which the PU supports to the VAU.

15) The VAU decides whether to start the transcoding process according to the media data format. The VAU starts the connection between PuID-ChannelNo, RecordNo and CallID and creates a RTSP Session NO.

16) The VAU sends a session response message to the M_CU.

17) The M_CU sends a RTSP TEARDOWN to the VAU in order to disconnect the real-time session.

18) The VAU sends a disconnect request to the PU to stop session.

19) The PU sends a disconnect response to the VAU to stop session.

20) The VAU sends a disconnect response to the M_CU to stop session.

7.3 PTZ control

The PTZ control function illustrated in Figure 7-4 is used to pan, tilt and zoom cameras, switch auxiliary peripherals (such as lighting, cooling fan and rain wipers) and to present the position of related physical devices.

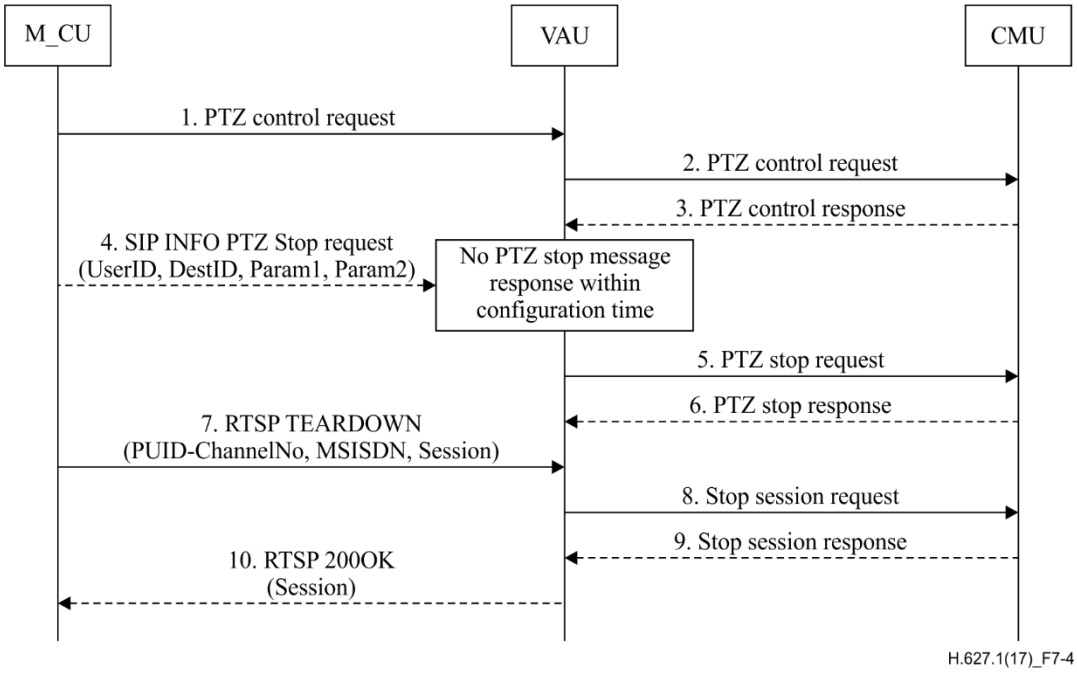

Figure 7-4 – PTZ control procedural flows

The message flows for PTZ control, illustrated in Figure 7-4, are as follows:

1) The M_CU sends a PTZ control request to the VAU. The message body carries UserID and DestID (DestID is PuID-ChannelNo).
2) The VAU sends a PTZ code to the CMU.
3) The CMU sends a PTZ control response to the VAU.
4) The M_CU sends a SIP INFO PTZ stop request to the VAU.
5) If the VAU receives the stop request from the M_CU within a specified time, the VAU sends a PTZ stop request to the CMU, otherwise, the VAU sends a PTZ stop request to the CMU automatically.
6) The CMU sends a PTZ stop response to the VAU.
7) The M_CU sends a RTSP TEARDOWN to the VAU in order to disconnect the real-time session.
8) The VAU sends the disconnect request to the CMU to stop session.
9) The CMU sends the disconnect response to the VAU to stop session.
10) The VAU sends the disconnect response to the M_CU to stop session.

7.4 Resource query

The message flows for a user resource query are illustrated in Figure 7-5.

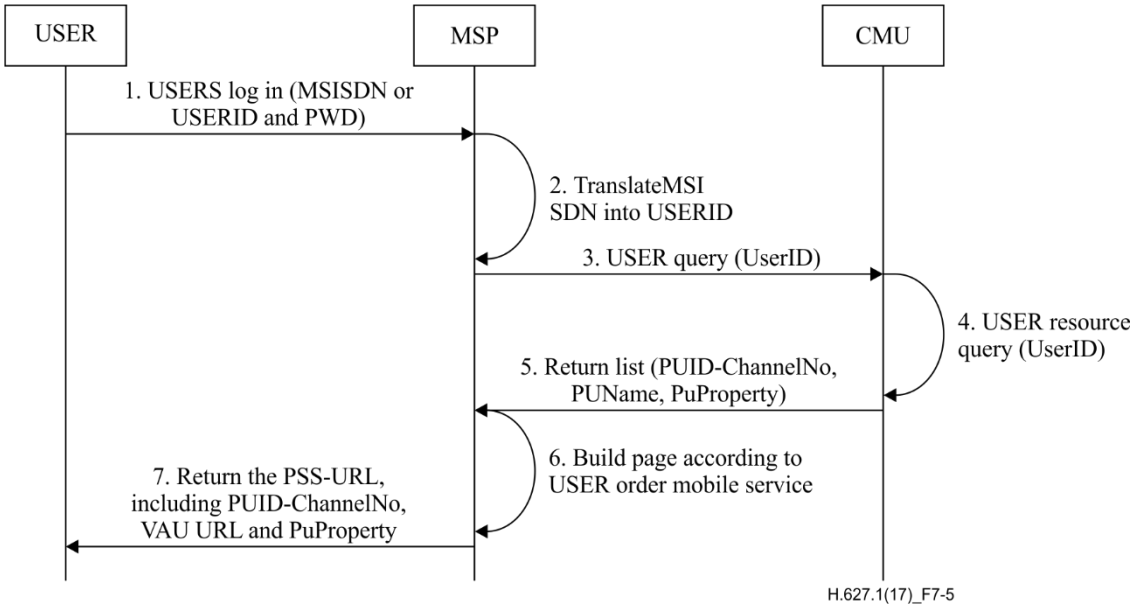

Figure 7-5 – User resource query procedural flows

The message flows for a user resource query, illustrated in Figure 7-5, are as follows:

1) USER logs into the MSP using MSISDN or USERID and password.
2) The MSP gets MSISDN-No from MSISDN, and then recognizes user type from MSISDN-No. Finally, the MSP translates the user type and MSISDN-No into UserID.
3) The MSP queries UserID in the CMU.
4) The CMU queries the user resource list according to UserID.
5) The CMU returns the list and user information to the MSP including PuID-ChannelNo, PUName, PuProperty.
6) The MSP builds a web page according to the user mobile service subscription.

7) The MSP returns the PSS-URL and user mobile service subscription.

7.5 Service management

7.5.1 VAU registration

The VAU registers to the CMU with its ID number and the capability information (including the transcoding and distribution capability) and re-registers automatically at regular times according to the configuration of the registration information. This is illustrated in Figure 7-6.

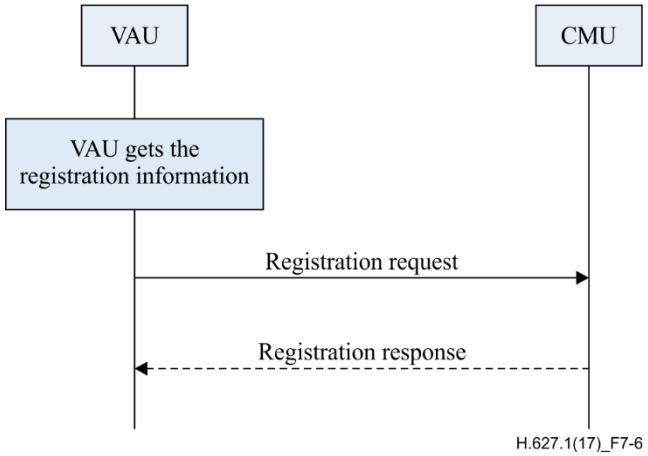

Figure 7-6 – VAU registration procedural flows

7.5.2 M_CU authorization

The M_CU sends a request to the MSP. The MSP gets the UserID and the password and sends an authorization request to the CMU. The CMU returns the ok information or the error code. This is illustrated in Figure 7-7.

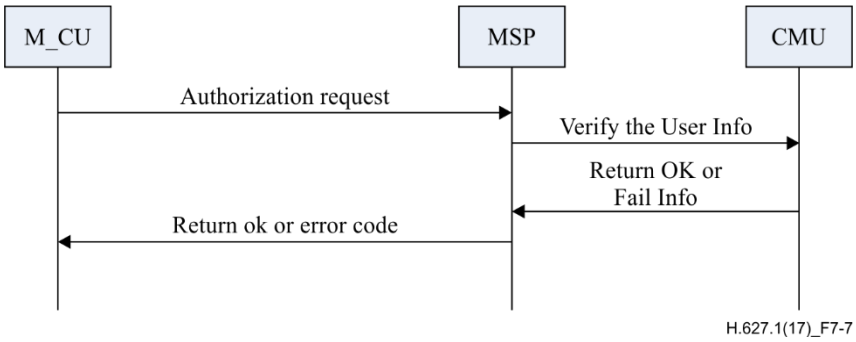

Figure 7-7 – M_CU authorization procedural flows

7.5.3 PU-related parameters query

The message flows for a PU-related query, illustrated in Figure 7-8, are as follows:

1) The MSP queries the source list of the current UserID.
2) The mobile CMU platform transfers the PU list and related information to the MSP. The information includes the PuID-ChannelNo, PUName and PuProperty.
3) The MSP processes the information and returns it to the M_CU for display.

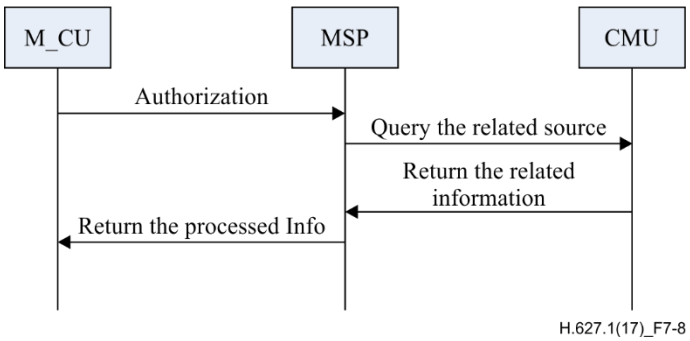

Figure 7-8 – Procedural flows for querying PU related parameters

Bibliography

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

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, 2017