International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.626.2

(12/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

Architecture for cloud storage in visual surveillance

Recommendation ITU-T H.626.2

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
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	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.626.2

Architecture for cloud storage in visual surveillance

Summary

Recommendation ITU-T H.626.2 defines a cloud storage architecture in visual surveillance. Cloud storage enables the service users to have ubiquitous, convenient and on-demand network access to a shared pool of the configurable storage resources, which can be rapidly provisioned and released with the minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance and its components are modularized and allocated dynamically based on the real usage. This Recommendation provides the architecture, entities, reference points and service control flow for cloud storage in visual surveillance.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.626.2	2017-12-14	16	11.1002/1000/13436

Keywords

Architecture, cloud storage, entity, reference point, service control flow, visual surveillance.

* 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.626.2

Architecture for cloud storage in visual surveillance

1 Scope

This Recommendation describes architecture, functional entities, reference points and service control flow of cloud storage in visual surveillance.

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

[ITU-T F.743.2] Recommendation ITU-T F.743.2 (2016), *Requirements for cloud storage in visual surveillance*.

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

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

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 cloud storage [ITU-T F.743.2]: A data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand.

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

3.1.4 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.

3.1.5 functional architecture [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 1 – 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 implementation and between administrative domains.

NOTE 2 – The definition is not only applicable to NGNs, but also to other IP packet switch based networks.

3.1.6 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

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

NOTE – An interface is defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges and other characteristics as appropriate.

3.1.8 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.

3.1.9 reference point [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.

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

3.1.11 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

This Recommendation defines the following terms:

3.2.1 cloud storage access unit (CSAU): A device located at a cloud storage system in visual surveillance. The CSAU is the key unit for implementing communication between the CSDU and the MDU, PU and the other media data related units defined in visual surveillance. The functions of the CSAU include service control function, media control function and configuration management function.

3.2.2 cloud storage data unit (CSDU): A series of devices located at a cloud storage system in visual surveillance. The CSDU is the data node in a cloud storage system that is used to store the massive multimodal data produced by the visual surveillance system. A typical visual surveillance cloud storage system consists of a number of CSDUs, which is organized in a distributed way. The CSDU can be dynamically extended according to the user's demand. The CSDU can receive the media data from the CSAU and write the data onto its local storage device. In addition, the CSDU can read and transmit the stored data to the CSAU according to the data reading requests.

3.2.3 cloud storage management unit (CSMU): A device located at the central part of a cloud storage system in visual surveillance. The CSMU is used to provide the management services of the cloud storage system and respond to the service requests of the visual surveillance system. The main functions of the CSMU include supporting storage resource management, data management, user management, service management, log management and security control.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CMU Centre Management Unit

CSAU Cloud Storage Access Unit

CSDU Cloud Storage Data Unit

CSMU Cloud Storage Management Unit

CU Customer Unit

IPU Intelligent Premises Unit

MDU Media Distribution Unit

MSU Media Storage Unit

NVR Network Video Recorder

PU Premises Unit

SCU Service Control Unit

VS Visual Surveillance

5 Conventions

None.

6 Overview of cloud storage in visual surveillance

The large-scale deployment of visual surveillance systems has contributed to the explosive growth of surveillance video data. It induces stringent needs for the efficient storage of massive video data and fast access of information of interest to users. Cloud storage is a data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In the cloud storage system, the physical and virtual resources can be dynamically assigned and reassigned according to the users' demands.

7 Functional architecture for cloud storage in visual surveillance

7.1 Architectural framework

Figure 7-1 shows the architectural framework for cloud storage in visual surveillance. The cloud storage based visual surveillance platform consists of two parts, which are respectively the traditional visual surveillance (VS) system and the cloud storage system. The cloud storage system can also be integrated with intelligent visual surveillance, mobile visual surveillance and other visual surveillance subsystems and the architecture is similar to that defined in this clause and is not described in this Recommendation.

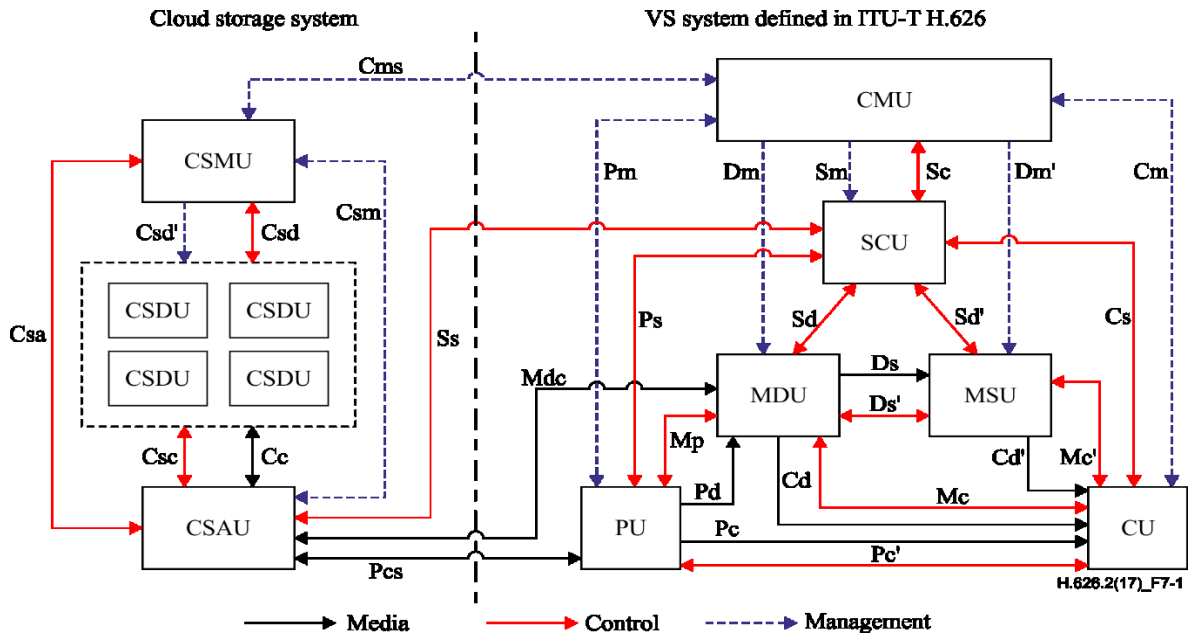

Figure 7-1 – Architectural framework for cloud storage in visual surveillance

The traditional VS service is a telecommunication service focusing on video (and audio) application technology, which is used to remotely capture multimedia (such as audio, video, image and various alarm signals) and present them to end users in a friendly manner (including accessibility aspects). The traditional VS system mainly includes six functional entities, which are the centre management unit (CMU), the service control unit (SCU), the media distribution unit (MDU), the media storage unit (MSU), the premises unit (PU) and the customer unit (CU). The function description of each functional entity is defined in [ITU-T H.626].

A visual surveillance cloud storage can provide a shared pool of configurable storage resources and related data storage functions to the VS applications. In a cloud storage system, the storage resources can be dynamically assigned and reassigned according to the users' demands. The cloud storage part mainly includes three functional entities, which are the cloud storage management unit (CSMU), the cloud storage data unit (CSDU) and the cloud storage access unit (CSAU).

– CSMU is used to provide the management services for the cloud storage system in the VS system.

– CSDU is the data node in a cloud storage system. A number of CSDUs are organized in a distributed way as a storage resource pool by using virtualization technology and the virtualized storage resource can be dynamically provided to the users on demand. The CSDUs are used to store the massive multimodal data produced by the VS system.

– CSAU is the key unit for implementing communication between the CSDU and the media data related units defined in the traditional VS system [ITU-T H.626]. The main functions of the CSAU include: receiving and responding to the control information of the CSMU, receiving and responding to the control information of the SCU, receiving the media data from MDU or PU, sending the media data to the MDU or other related visual surveillance entities, writing the media data into the CSDU cluster and reading the media data from the CSDU cluster.

7.2 Functional entities

7.2.1 Cloud storage management unit

The cloud storage management unit (CSMU) is used to provide the management services for the cloud storage system and respond to service requests of the VS system. The main functions of the

CSMU include storage resource management, data management, user management, service management, log management and security control. The CSMU is used to achieve collaboration among the different storage devices and guarantee better access performance of the multimodal surveillance data.

7.2.2 Cloud storage data unit

The cloud storage data unit (CSDU) is the data node in a cloud storage system which is used to store the massive multimodal data produced by the VS system. A typical visual surveillance cloud storage system has a number of CSDUs, which are organized in a distributed way as a storage resource pool by using virtualization technology. The CSDU can be dynamically extended according to the user's demand and the virtualized storage resource can be dynamically provided to the users on demand. The CSDU can receive media data from the CSAU and write the data onto its local storage device. In addition, the CSDU can read and transmit the stored data to the CSAU according to the data reading requests.

7.2.3 Cloud storage access unit

The cloud storage access unit (CSAU) is the key unit for implementing communication between the CSDU and the media data related units defined in the VS system [ITU-T H.626]. As shown in Figure 7-2, the functions of the CSAU are divided into three categories, which are the service control function, the media control function and the configuration management function.

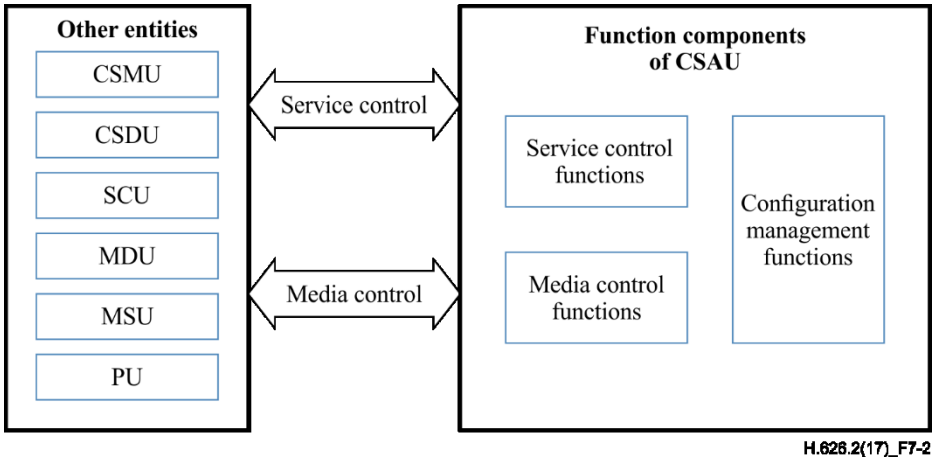

Figure 7-2 – Function components of CSAU

Service control function

– initiate, maintain and release the connection with the SCU;

– process the service requests from the CSMU, forward them to the SCU and respond to the CSMU.

Media control function

– receive media data from the MDU, the PU, the MSU and/or other data source entities of the VS system;

– transmit or forward media data into the CSDU cluster;

– receive media data distributed in the CSDU cluster;

– transmit or forward media data to the MDU, the CU and/or other related entities of the VS system.

Configuration management function

– manage the overall configuration in the CSAU, including the service control, data transmission and other media storage control.

7.3 Reference points

7.3.1 Reference point Pcs: PU-CSAU

The reference point Pcs is located between the PU and the CSAU. It is used to deliver the media data directly from the PU to the CSAU according to the media storage requests.

7.3.2 Reference point Mdc: MDU-CSAU

The reference point Mdc is located between the MDU and the CSAU. It is used for the media data transmission between the MDU and the CSAU according to the media reading and writing requests.

7.3.3 Reference point Ss: CSAU-SCU

The reference point Ss is located between the CSAU and the SCU. It is used to control the CSAU registration, access authentication, authorization and accounting by the SCU and is used for the control signal transmission between the CSAU and the SCU.

7.3.4 Reference point Cms: CMU-CSMU

The reference point Cms is located between the CMU and the CSMU. It is used for the management signal transmission between the CMU and the CSMU.

7.3.5 Reference point Csm: CSMU-CSAU

The reference point Csm is located between the CSMU and the CSAU. It is used by the CSMU to manage the service control function, the media control function and the configuration management function of the CSAU.

7.3.6 Reference point Csd: CSMU-CSDU

The reference point Csd is located between the CSMU and the CSDU. It is used for the control signal transmission between the CSMU and the CSDU.

7.3.7 Reference point Csd': CSMU-CSDU

The reference point Csd' is located between the CSMU and the CSDU. It is used to support the storage space management. The main functions are as follows.

– increase or decrease the storage space flexibly according to the users' demands;

– support data management in the CSDU, including data addition, data deletion, data browsing and data retrieval, etc.

7.3.8 Reference point Csc: CSDU-CSAU

The reference point Csc is located between the CSDU and the CSAU. It is used for the media access control signal transmission between the CSAU and the CSDU.

7.3.9 Reference point Cc: CSDU-CSAU

The reference point Cc is located between the CSAU and the CSDU. It is used for the media data transmission between the CSAU and the CSDU.

7.3.10 Reference point Csa: CSMU-CSAU

The reference point Csa is located between the CSAU and the CSMU. It is used for the access control signal transmission between the CSMU and the CSAU.

7.4 Service control flow

7.4.1 Real-time media storage

When a user wants to store the real-time media obtained from the PU into the cloud storage system, the CU initiates a storage request and sends it to the SCU to start the media storage.

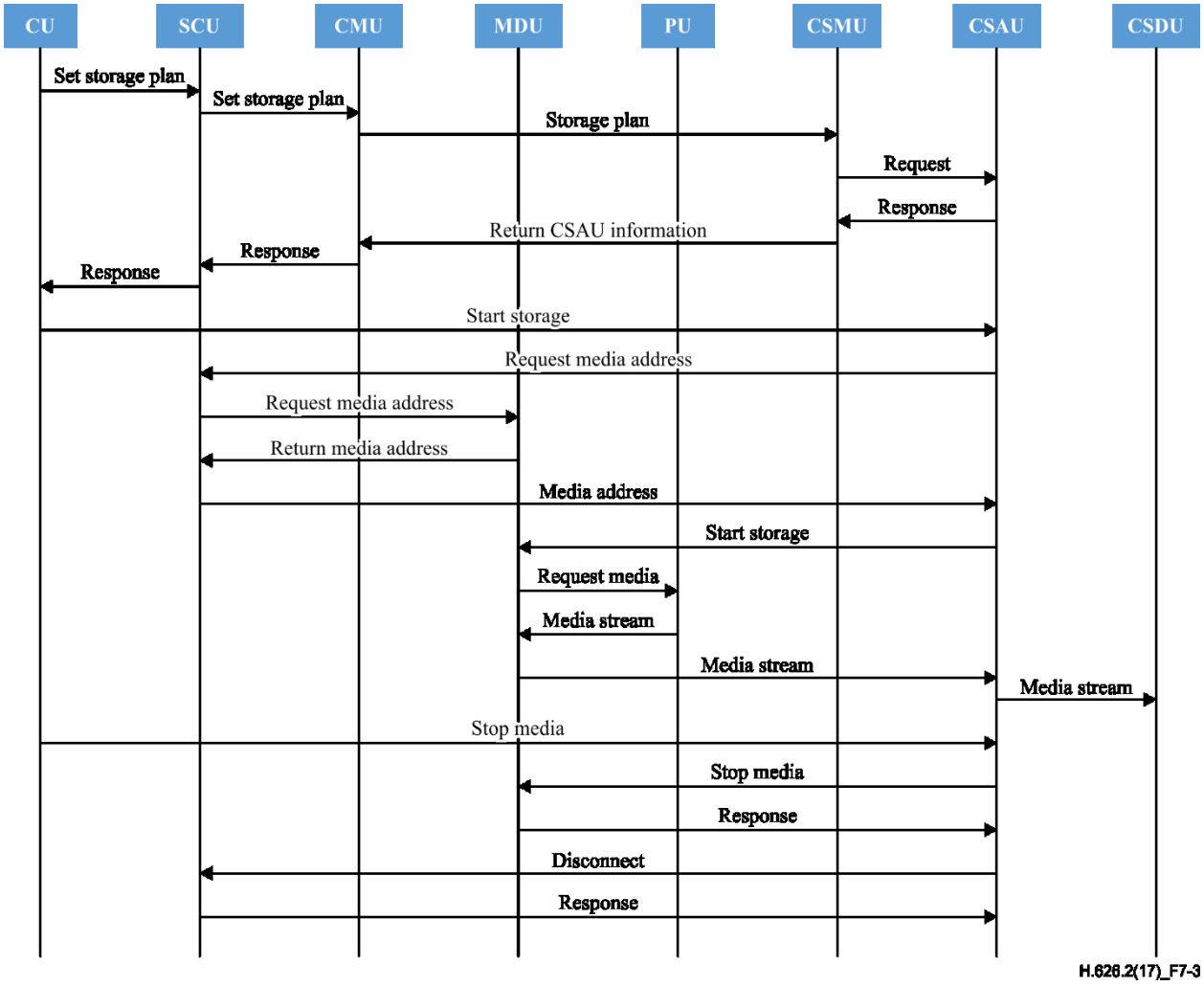

Figure 7-3 – High-level procedural flows for real-time media storage

Figure 7-3 shows the procedural flows of real-time media storage in a cloud storage system:

(1) The CU initiates a storage plan request and sends this request to the SCU.

(2) The SCU forwards this storage plan request to the CMU.

(3) The CMU authenticates the storage access permission and then sends this storage plan request to the CSMU.

(4) The CSMU authenticates the storage access permission and then sends this storage plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this storage plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response including the CSAU information to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the real-time media storage request to the CSAU.

(10) When the CSAU receives the storage request, it sends a request to the SCU for the media address.

(11) The SCU forwards this request to the MDU.

(12) The MDU returns the media address to the SCU.

(13) The SCU transfers the media address to the CSAU.

(14) After receiving the real-time media address, the CSAU requests the MDU to start transmitting the media stream.

(15) The MDU sends a request to the PU for initiating a media stream.

(16) The PU creates a media channel with the MDU and sends the media stream to the MDU.

(17) The MDU transfers the media stream to the CSAU.

(18) The CSAU transfers this media stream to the CSDU to store it in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop-media request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this real-time media storage.

7.4.2 Video file storage

A network video recorder (NVR) is usually used as a typical MSU for continuously recording the surveillance video from network cameras. When a user wants to upload a video file from the NVR to the cloud storage system, the CU initiates a storage request and sends it to the SCU to start the media storage.

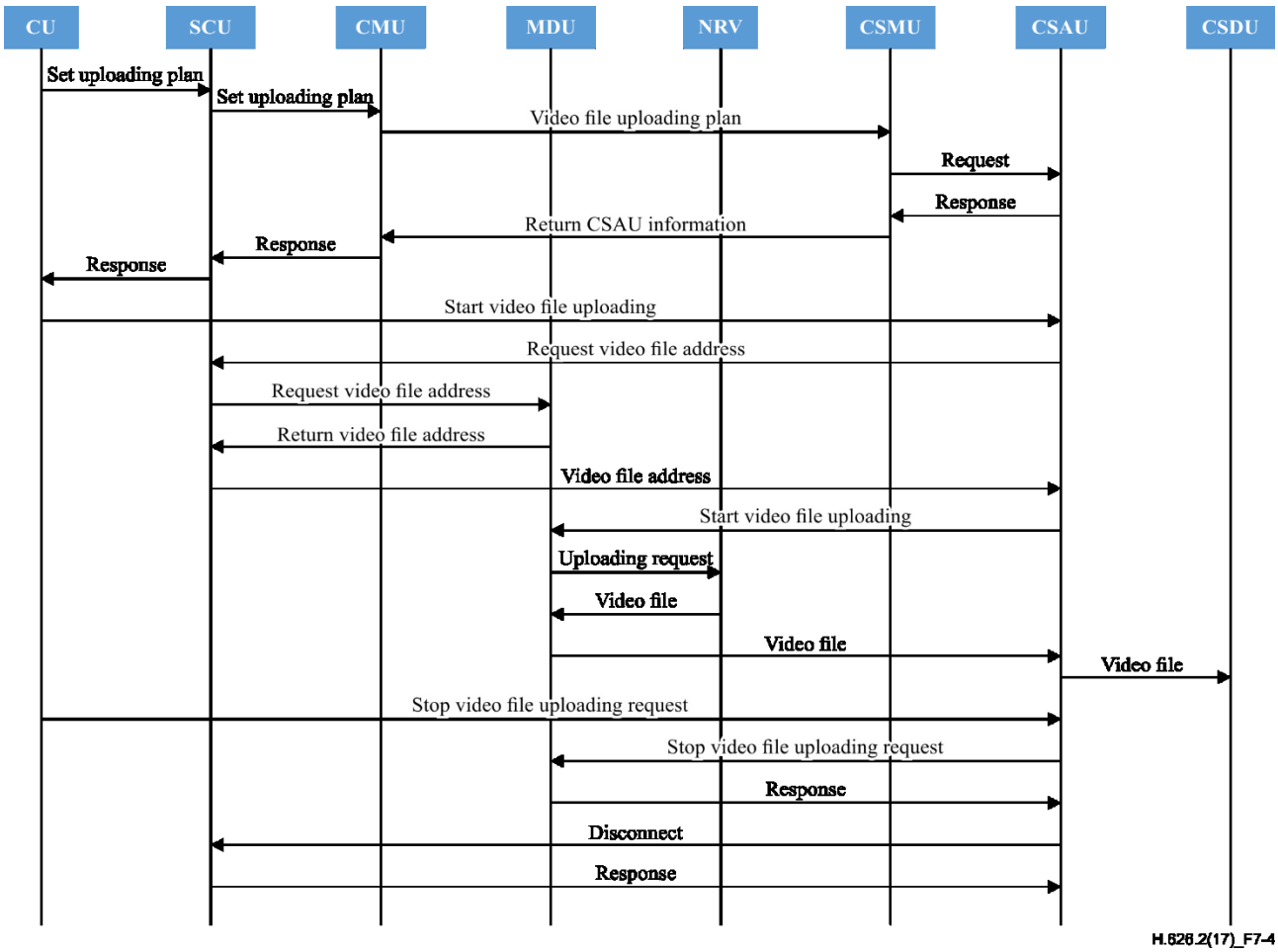

Figure 7-4 – High-level procedural flows for video file uploading from NVR

Figure 7-4 shows the procedural flows of video file uploading from the NVR to the cloud storage system:

(1) The CU initiates a video file uploading plan request and sends this request to the SCU.

(2) The SCU forwards this uploading plan request to the CMU.

(3) The CMU authenticates the uploading access permission and then sends this uploading plan request to the CSMU.

(4) The CSMU authenticates the uploading access permission and then sends this uploading plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this video file uploading plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the video file uploading request to the CSAU.

(10) When the CSAU receives the uploading request, it sends a request to the SCU for the data source address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the file address to the SCU.

(13) The SCU transfers the file address to the CSAU.

(14) After receiving the file address, the CSAU requests the MDU to start video file uploading from the NVR.

(15) The MDU sends a request to the NVR for obtaining the video files.

(16) The NVR creates a video transmission channel with the MDU and sends the video files to the MDU.

(17) Then MDU transfers the video files to the CSAU.

(18) The CSAU transfers the video files to the CSDU to store them in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop-media request to the MDU.

(21) Then MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this video file uploading.

7.4.3 Image storage

The network cameras continuously capture images. When a user wants to store these images directly into the cloud storage system, the CU initiates a request to the SCU to start the image storage.

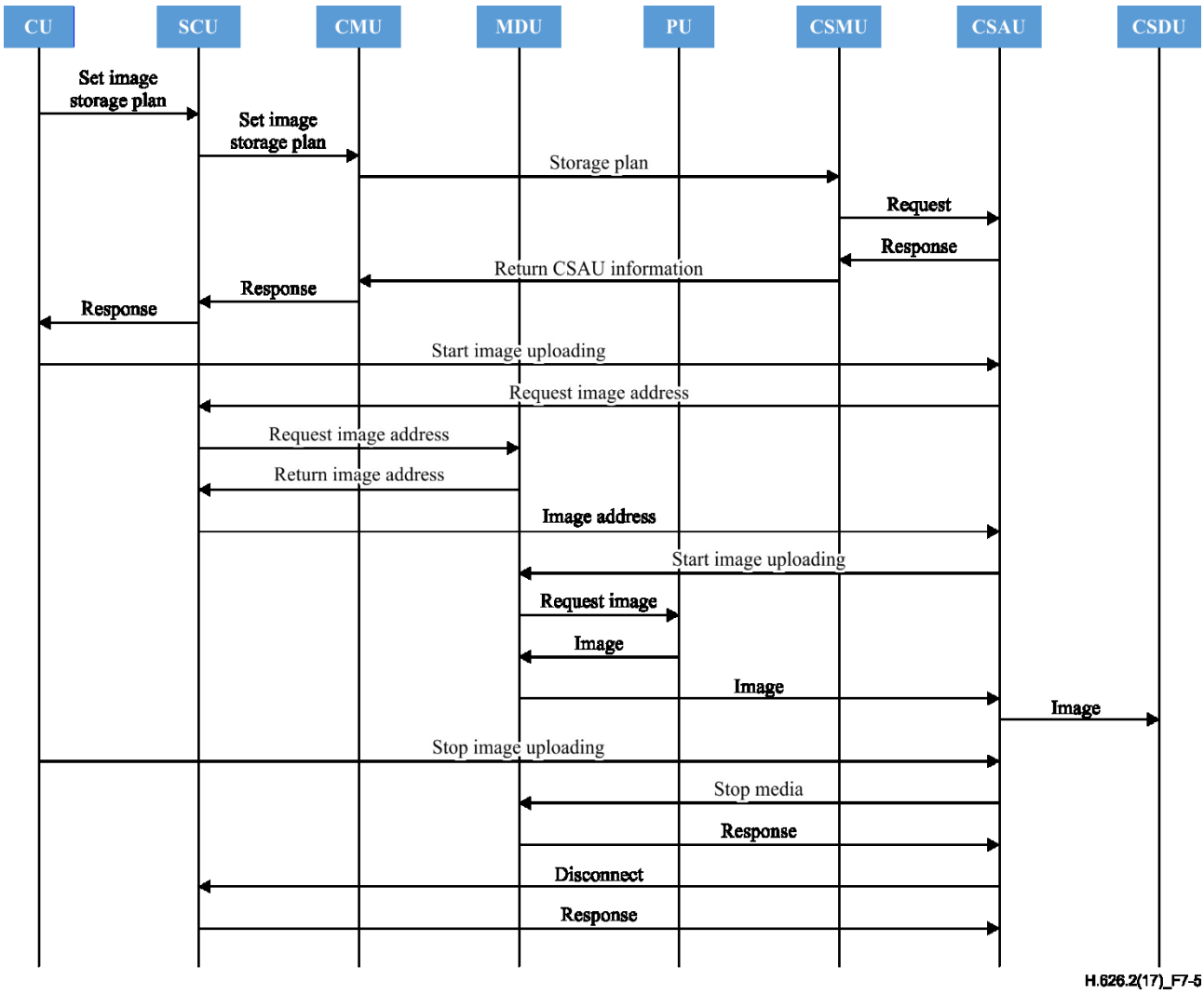

Figure 7-5 – High-level procedural flows for image uploading from surveillance camera

Figure 7-5 shows the procedural flows of the image uploading from the PU to the cloud storage system:

(1) The CU initiates an image storage request and sends this request to the SCU.

(2) The SCU forwards this image uploading plan request to the CMU.

(3) The CMU authenticates the uploading access permission and then sends this uploading plan request to the CSMU.

(4) The CSMU authenticates the uploading access permission and then sends this uploading plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this uploading plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the image storage request to the CSAU.

(10) When the CSAU receives the request, it sends a request to the SCU for the data source address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the address to the SCU.

(13) The SCU transfers the data source address to the CSAU.

(14) After receiving the data source address, the CSAU requests the MDU to start the image uploading from the PU.

(15) The MDU sends a request to the PU for obtaining the captured images.

(16) The PU creates an image transmission channel with the MDU and sends the captured images to the MDU.

(17) The MDU transfers the images to the CSAU.

(18) The CSAU transfers the images to the CSDU to store the received images in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end the image uploading from the PU.

7.4.4 Video metadata or image metadata storage

The intelligent visual surveillance system can provide various intelligent services by using video or image analysis technologies. One solution is to implement some intelligent visual analysis algorithms in the PU that is defined as the intelligent premises unit (IPU). When a user wants to store video metadata or image metadata extracted from the original video or image data in the cloud storage system, the CU initiates a request to the SCU to start this procedure.

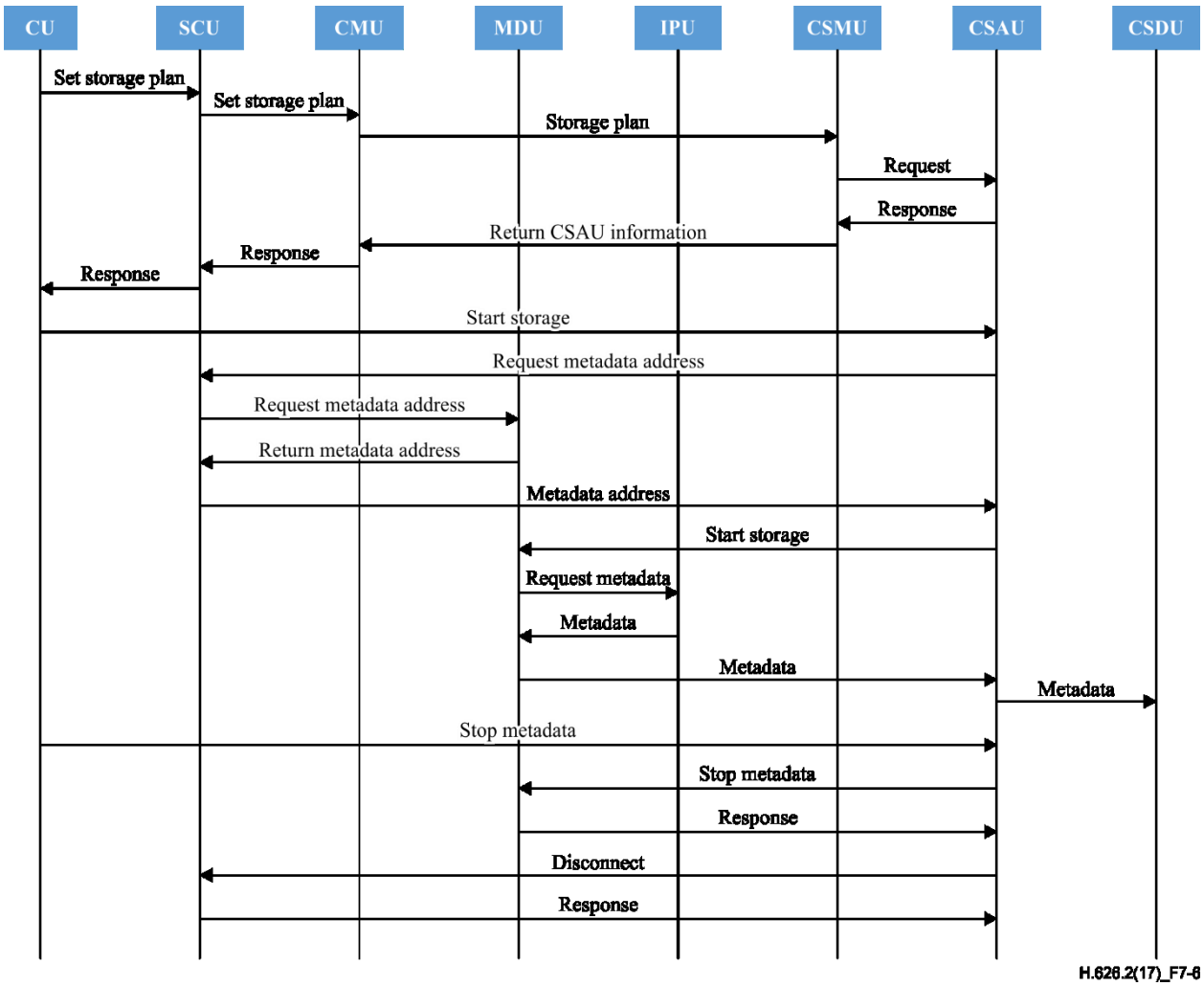

Figure 7-6 – High-level procedural flows for video metadata or image metadata storage

Figure 7-6 shows the procedural flows of the video metadata or image metadata storage in cloud storage system:

(1) The CU initiates a storage plan request and sends this request to the SCU.

(2) The SCU forwards this storage plan request to the CMU.

(3) The CMU authenticates the storage access permission and then sends this storage plan request to the CSMU.

(4) The CSMU authenticates the storage access permission and then sends this storage plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this storage plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the video metadata or image metadata storage request to the CSAU.

(10) When the CSAU receives the storage request, it sends a request to the SCU for the metadata address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the metadata address to the SCU.

(13) The SCU transfers the metadata address to the CSAU.

(14) After receiving the metadata address, the CSAU requests the MDU to start transmitting the metadata.

(15) The MDU sends a request to the IPU for the video metadata or image metadata.

(16) The IPU creates a media channel with the MDU and sends the metadata to the MDU.

(17) The MDU transfers the metadata to the CSAU.

(18) The CSAU transfers the metadata to the CSDU to store it in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this metadata storage.

7.4.5 Media acquisition from the cloud storage system

When a user wants to view the media stored in a cloud storage system, the CU initiates a request to the SCU in order to acquire the media.

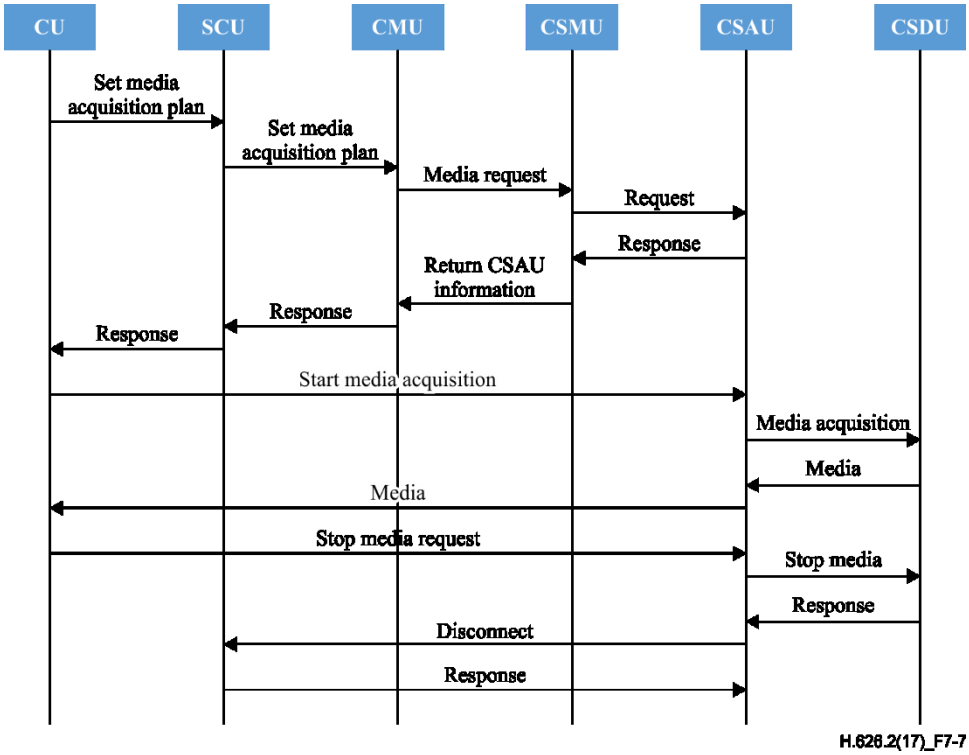

Figure 7-7 – High-level procedural flows for media acquisition

Figure 7-7 shows the procedural flows of the media acquisition from the cloud storage system to the CU:

(1) The CU initiates a media acquisition request and sends this request to the SCU.

(2) The SCU forwards this acquisition request to the CMU.

(3) The CMU authenticates the acquisition access permission and then sends this request to the CSMU.

(4) The CSMU authenticates the acquisition access permission and then sends this request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this media acquisition request.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the response, it sends a media acquisition request to the CSAU.

(10) The CSAU transfers this request to the CSDU.

(11) After receiving this request, the CSDU creates a media channel with the CSAU to transmit the required media data.

(12) The CSAU transfers the media data to the CU.

(13) When the CU stops the media acquisition, it sends a stop request to the CSAU.

(14) The CSAU transfers this request to the CSDU.

(15) The CSDU returns a response to the CSAU.

(16) The CSAU requests the SCU to disconnect.

(17) The SCU returns a response to end this media acquisition operation.

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, 2018