International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.743.8

(05/2019)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Multimedia services

# Requirements for a cloud computing platform supporting a visual surveillance system

Recommendation ITU-T F.743.8

ITU-T F-SERIES RECOMMENDATIONS

**NON-TELEPHONE TELECOMMUNICATION SERVICES**

| | |
|---|---|
| TELEGRAPH SERVICE | |
| Operating methods for the international public telegram service | F.1–F.19 |
| The gentex network | F.20–F.29 |
| Message switching | F.30–F.39 |
| The international telemessage service | F.40–F.58 |
| The international telex service | F.59–F.89 |
| Statistics and publications on international telegraph services | F.90–F.99 |
| Scheduled and leased communication services | F.100–F.104 |
| Phototelegraph service | F.105–F.109 |
| MOBILE SERVICE | |
| Mobile services and multidestination satellite services | F.110–F.159 |
| TELEMATIC SERVICES | |
| Public facsimile service | F.160–F.199 |
| Teletex service | F.200–F.299 |
| Videotex service | F.300–F.349 |
| General provisions for telematic services | F.350–F.399 |
| MESSAGE HANDLING SERVICES | F.400–F.499 |
| DIRECTORY SERVICES | F.500–F.549 |
| DOCUMENT COMMUNICATION | |
| Document communication | F.550–F.579 |
| Programming communication interfaces | F.580–F.599 |
| DATA TRANSMISSION SERVICES | F.600–F.699 |
| **MULTIMEDIA SERVICES** | **F.700–F.799** |
| ISDN SERVICES | F.800–F.849 |
| UNIVERSAL PERSONAL TELECOMMUNICATION | F.850–F.899 |
| ACCESSIBILITY AND HUMAN FACTORS | F.900–F.999 |

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

# Recommendation ITU-T F.743.8

## Requirements for a cloud computing platform supporting a visual surveillance system


### Summary

Recommendation ITU-T F.743.8 specifies the requirements for a cloud computing platform supporting visual surveillance. Cloud computing is an emerging technology aimed at providing various computing services over the Internet. Using virtualization technology, a cloud computing platform realizes a ubiquitous and flexible shared resources pool that can be rapidly provisioned and released with minimal management effort or service-provider interaction based on the needs of users. By using the cloud computing technology, the visual surveillance system can conveniently manage various functional components and services, such as video distribution, video transcoding and intelligent video processing. This Recommendation provides the application scenarios and requirements for a cloud computing platform supporting a visual surveillance system.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T F.743.8 | 2019-05-14 | 16 | 11.1002/1000/13898 |

### Keywords

Cloud computing, requirements, scenarios, 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


| | | Page |
|---|---|---|
| 1 | Scope | 1 |
| 2 | References | 1 |
| 3 | Definitions | 1 |
| | 3.1 Terms defined elsewhere | 1 |
| | 3.2 Terms defined in this Recommendation | 1 |
| 4 | Abbreviations and acronyms | 1 |
| 5 | Conventions | 2 |
| 6 | Scenarios | 2 |
| | 6.1 Video distribution | 2 |
| | 6.2 Video transcoding | 2 |
| | 6.3 Online intelligent video processing | 3 |
| | 6.4 Offline intelligent video processing | 4 |
| 7 | Requirements for cloud computing platform supporting visual surveillance | 5 |
| | 7.1 User requirements | 5 |
| | 7.2 Service requirements | 5 |
| | 7.3 Security requirements | 6 |
| | 7.4 Management requirements | 7 |
| | 7.5 Scalability requirements | 7 |
| | 7.6 Reliability requirements | 8 |
| | 7.7 Performance requirements | 8 |
| Bibliography | | 9 |

# Recommendation ITU-T F.743.8

## Requirements for a cloud computing platform supporting a visual surveillance system

### 1 Scope

This Recommendation specifies the application scenarios and requirements for a cloud computing platform supporting a visual surveillance system.

### 2 References

None.

### 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 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.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

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

**3.1.6 premises unit** [b-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.

**3.1.7 visual surveillance** [b-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 signals, 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:

CU Customer Unit

IVS Intelligent Visual Surveillance

MCU Mobile Customer Unit

MSU Media Storage Unit

PU Premises Unit

VS Visual Surveillance

VSCC Visual Surveillance Cloud Computing

## 5 Conventions

In this Recommendation:

– 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.

## 6 Scenarios

This clause describes typical scenarios illustrating the cloud computing platform supporting visual surveillance and deriving its service requirements.

### 6.1 Video distribution

The cloud computing platform in a visual surveillance (VS) system can support large-scale real-time video forwarding. For example, many surveillance cameras are deployed in the Great Wall Scenic Area, and the remote monitoring function of the cameras is open to the public. If users wants to see current images of the Great Wall remotely, they can view the network video information on their local devices through the cloud-based real-time video distribution function.

Step 1: Users enter the customer unit (CU) which supports remote live video viewing of the Great Wall Scenic Area, and submit their request to the VS system.

Step 2: After receiving a video-viewing request, the VS system authenticates the user information, and obtains the related information from a video-forwarding function unit that is deployed on the cloud computing platform. The cloud computing platform can dynamically create or destroy the video-forwarding function according to current user requests. The VS system then responds to the CU with the information about the video-forwarding function on the cloud computing platform.

Step 3: After receiving the VS system response, the CU sends a video-viewing request to the cloud computing platform.

Step 4: The cloud computing platform obtains the video stream from the corresponding camera, and then forwards the video stream to the CU.

### 6.2 Video transcoding

The cloud computing platform in a VS system can support video-transcoding functions, e.g., code rate transformation and video format conversion. The traffic department of a city has deployed a large-scale VS system in the city streets with high-definition network cameras. Users want to view the current traffic situation on their way home with their mobile phones. Due to the limited bandwidth of mobile devices and mobile data traffic limits, high-definition surveillance video needs to be transcoded to low-resolution video before forwarding to the CU. The video-transcoding operation can be carried out on the cloud computing platform.

Step 1: Users log into the VS system via their mobile customer unit (MCU), and select the appropriate network camera. The MCU then sends a video-viewing request to the VS system with the video format description.

Step 2: After receiving the video-viewing request, the VS system authenticates the user information, and obtains the related information from a video-forwarding function unit that is deployed on the cloud computing platform. The VS system then responds to the MCU with the information from the video-forwarding function in the cloud computing platform.

Step 3: After receiving the response of the VS system, the MCU sends a video-viewing request to the cloud computing platform.

Step 4: The cloud computing platform obtains the video stream from the corresponding camera. Then, according to the video format description of the MCU, the surveillance video stream is transcoded by the video-transcoding component deployed in the cloud computing platform. The cloud computing platform can dynamically create and destroy the video-forwarding function according to the current requests of the MCU. After that, the transcoded video stream is sent to the MCU.

## 6.3 Online intelligent video processing

### 6.3.1 Case 1: Traffic flow analysis

The traffic department of a city has deployed an intelligent visual surveillance (IVS) system for city roads. The system administrator is responsible for operating the IVS system to carry out traffic management tasks. The work of the administrator is to monitor real-time traffic flow of key road sections in the traffic rush hour. A traffic flow analysis function can be developed based on computer vision technology, and is virtualized as functional components in the cloud computing platform. When a user needs to obtain the traffic flow situation of certain road sections, the system can call the traffic flow analysis function to process the relevant surveillance video streams.

Step 1: Users log into the IVS system through the CU. They choose certain surveillance cameras that are deployed on key road sections of interest and set the traffic flow analysis function. They then submit traffic flow analysis requests to the IVS system.

Step 2: After receiving the traffic flow analysis request, the IVS system authenticates the user information, and obtains the relevant information from the traffic flow analysis function that is deployed on the cloud computing platform. The cloud computing platform can dynamically create and destroy the traffic flow analysis function components according to current user requests. The IVS system then responds to the CU with the information from the traffic flow analysis function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform obtains the relevant video streams from the corresponding cameras, online processes the video streams and then sends the real-time traffic flow analysis results back to the CU.

### 6.3.2 Case 2: Perimeter prevention

An electricity company uses an IVS system to monitor key power transmission equipment deployed in a city. Surveillance cameras are deployed around the power transmission equipment and the IVS system online analyses the captured surveillance video by calling the perimeter prevention function. Once someone approaches the power transmission equipment, the IVS system generates an alarm message to alert the user to the exception. The perimeter prevention function is virtualized as functional components in the cloud computing platform, and can be dynamically created and destroyed according to current user requests. The working step of the online perimeter prevention scenario is similar to that of the online traffic flow analysis scenario.

## 6.4 Offline intelligent video processing

### 6.4.1 Case 1: Human recognition

A public security department has deployed an IVS system in a city street. The system administrator is responsible for operating the IVS system to carry out public security tasks. When there is a robbery in front of a bank, the administrator reviews the relevant surveillance video captured by the cameras deployed around the bank and obtains a picture of the robber. To find the escape route of the robber as soon as possible, the administrator uses the intelligent human recognition function of the IVS system to process the massive related historical surveillance video. The intelligent human recognition function can be virtualized as functional components in the cloud computing platform and can be dynamically created according to user demand.

Step 1: Users log into the IVS system through the CU. To quickly find robber information in the massive surveillance video data, the user needs to set several functional parameters, such as the camera channel numbers, the time period of interest in the historical video and the picture of the robber, and then sends an intelligent human recognition request to the IVS system.

Step 2: After receiving the human recognition request, the IVS system authenticates the user information, requests the cloud computing platform to create the intelligent human recognition function, and then responds to the CU with the information from the intelligent human recognition function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform downloads the relevant video files from the media storage unit (MSU), processes the video files in parallel and then sends the human recognition results back to the CU.

Step 5: When the intelligent human recognition task finishes, the cloud computing platform destroys the intelligent human recognition function to release the corresponding resources.

### 6.4.2 Case 2: Video synopsis

The IVS system deployed by a public security department produces massive surveillance video continuously and the cost of data storage is high. However, the public security department is usually interested in moving objects in the surveillance video. Therefore, to save storage space, surveillance video is usually processed to generate synopsis video before long-term storage. The objective of video synopsis is to shorten the video time by reorganizing moving video objects in temporal and spatial dimensions. For example, by using the video synopsis operation, a 24 h surveillance video file is transformed into a 30 min video file that contains all moving objects in the original video file. The intelligent video synopsis function can be virtualized as functional components in the cloud computing platform, and can be dynamically created according to user demand.

Step 1: Users log into the IVS system through the CU, and set several functional parameters of the video synopsis, such as the camera channel numbers, the time period of interest in the historical video and the density of the objects. Then users send an intelligent video synopsis request to the IVS system.

Step 2: After receiving the video synopsis request, the IVS system authenticates the user information, requests the cloud computing platform to create the intelligent video synopsis function and then responds to the CU with the information from the intelligent video synopsis function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform downloads the relevant video files from the MSU, processes the video files in parallel and then uploads the video synopsis results back to the MSU.

Step 5: When the intelligent video synopsis task finishes, the cloud computing platform destroys the intelligent video synopsis function to release the corresponding resources.

# 7 Requirements for cloud computing platform supporting visual surveillance

## 7.1 User requirements

There are two types of user: cloud computing service consumers and cloud computing service providers.

### 7.1.1 Cloud computing service consumer requirements

– USR-01: A visual surveillance cloud computing (VSCC) platform is required to support registration and de-registration of the end user through the interface provided by the system and the end user can view and modify personal information.

– USR-02: A VSCC platform is required to support convenient end-user login to and logout from the system. A username and password are required when an end user logs into the system.

– USR-03: A VSCC platform is recommended to support end-user view of the user access logs or other system logs.

– USR-04: A VSCC platform is recommended to support real-time surveillance video distribution.

– USR-05: A VSCC platform is recommended to support the online or offline surveillance video-transcoding function.

– USR-06: A VSCC platform is recommended to support online or offline intelligent surveillance video analysis functions.

– USR-07: A VSCC platform is required to support the configuration of computing resources for video surveillance tasks on demand.

– USR-08: A VSCC platform is required to support the user view of the status of user computing tasks and computing resources.

### 7.1.2 Cloud computing service provider requirements

– USR-09: A VSCC platform is required to support convenient provider login to and logout from the system. The provider name and password are required when logging into the system.

– USR-10: A VSCC platform is required to support the provider view of the system operating status from the beginning to now, including the system computing resource occupancy rate, the remaining computing resources of the system, the computing resource occupancy rate of individual users and the remaining computing resources of individual users.

– USR-11: A VSCC platform is required to support flexible computing resource assignment for individual users.

## 7.2 Service requirements

### 7.2.1 Online intelligent video processing service requirements

– SER-01: A VSCC platform is recommended to support online intelligent video processing. The video processing components deployed on a VSCC platform can receive video streams from premises units (PUs) and process the video in real time.

– SER-02: A VSCC platform is recommended to support online management of video processing tasks, such as creation, pause, restart and deletion.

– SER-03: A VSCC platform is recommended to view the progress of online video processing tasks.

– SER-04: A VSCC platform is recommended to view the status of resources utilized by online intelligent video processing tasks.
– SER-05: A VSCC platform is recommended to support the viewing of log files that record the operations of online intelligent video processing tasks.

### 7.2.2 Offline intelligent video processing service requirements

– SER-06: A VSCC platform is recommended to support offline intelligent video processing. The video processing components deployed on the VSCC platform can download the video files from the MSU and carry out their batch processing.
– SER-07: A VSCC platform is recommended to support offline management of video processing tasks, such as creation, pause, restart and deletion.
– SER-08: A VSCC platform is recommended to view the progress of offline video processing tasks.
– SER-09: A VSCC platform is recommended to view the status of resources utilized by offline intelligent video processing tasks.
– SER-10: A VSCC platform is recommended to support the viewing of log files that record the operations of offline intelligent video processing tasks.

### 7.2.3 Video transcoding

– SER-11: A VSCC platform is recommended to support video transcoding. The video-transcoding components deployed on the VSCC platform can receive video streams from PUs and transcode the video in real time. In addition, the video-transcoding components can download video files from the MSU and carry out their transcoding in batches.
– SER-12: A VSCC platform is recommended to support the management of video-transcoding tasks, e.g., creation, pause, restart and deletion.
– SER-13: A VSCC platform is recommended to view the progress of video-transcoding tasks.
– SER-14: A VSCC platform is recommended to view the status of resources utilized by video-transcoding tasks.
– SER-15: A VSCC platform is recommended to support the viewing of log files that record the operations of video-transcoding tasks.

## 7.3 Security requirements

### 7.3.1 Authentication security requirements

– SEC-01: A VSCC platform is required to provide the mechanisms for authentication and authorization, and to permit only authorized users to access the system and use system services. A VSCC platform is required to forbid unauthorized users to handle any system resources.

### 7.3.2 Access security requirements

– SEC-02: A VSCC platform is required to operate in an environment where network address translation (NAT) or firewall devices are present. It is recommended to utilize specified firewalls, gatekeepers and other network devices to ensure security for access to some special cloud computing services.

### 7.3.3 Content security requirements

– SEC-03: A VSCC platform is recommended to ensure the security of processed video data, the results of the video processing, etc.
– SEC-04: A VSCC platform is required to protect user privacy.

### 7.3.4 System security requirements

– SEC-05: A VSCC platform is required to have the capability to resist various attacks.

– SEC-06: A VSCC platform is required to provide troubleshooting mechanisms. It is required that a structural single-node problem be avoided (i.e., a problem at a single node should not cause failure of the entire system).

## 7.4 Management requirements

### 7.4.1 Resources management requirements

– MAN-01: A VSCC platform is required to support resource management of the cloud computing platform. Resources can be increased and decreased flexibly according to service requests.

### 7.4.2 Equipment management requirements

– MAN-02: A VSCC platform is required to provide unified management of the computing equipment.

### 7.4.3 Service management requirements

– MAN-03: A VSCC platform is required to provide various computing service subscription means for users, and to provide the capabilities to query, view and modify their subscription information.

– MAN-04: A VSCC platform is recommended to provide the capability of accounting, charging and billing for the computing service operation.

– MAN-05: A VSCC platform is recommended to provide various alternative accounting modes, and to support flexible combination of payment modes, billing modes, billing cycles, preferential pricing, etc.

### 7.4.4 System management requirements

– MAN-06: A VSCC platform is required to provide a unified system management interface that can be called conveniently.

– MAN-07: A VSCC platform is required to provide a visual interface for users.

### 7.4.5 Operation management requirements

– MAN-08: A VSCC platform is required to monitor, record and display the running status of the system.

– MAN-09: A VSCC platform is required to monitor, record and display usage of cloud computing cluster resources.

## 7.5 Scalability requirements

– SCA-01: A VSCC platform is required to provide computing resource scalability. When computing equipment is increased or decreased in the system, the computing capacity of the VSCC platform is increased or decreased accordingly, and the system service is uninterrupted.

– SCA-02: A VSCC platform is required to provide computing resources scalability for users. The computing resources of individual users can be increased or decreased according to each user's demand.

– SCA-03: A VSCC platform is required to provide user scalability. The number of supported users can be increased or decreased dynamically.

### 7.6 Reliability requirements

– REL-01: A VSCC platform is required to ensure service reliability. When computing equipment fails or the system network operation is abnormal, the system service can be used normally.

### 7.7 Performance requirements

– PER-01: A VSCC platform is required to support concurrent user operations. The system can serve a large number of users simultaneously, while ensuring service quality.

# Bibliography


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

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

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

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

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

## 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, 2019