ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Supplement

ITU-T J Suppl. 13 (11/2023)

SERIES J: Cable networks and transmission of television, sound programme and other multimedia signals

Supplements to ITU-T J-series Recommendations

ITU-T J.1036 – Factual subscriber-base reporting and protected content delivery in conditional access system – Test methods

ITU-T J-SERIES RECOMMENDATIONS

Cable networks and transmission of television, sound programme and other multimedia signals

GENERAL RECOMMENDATIONS	J.1-J.9
GENERAL SPECIFICATIONS FOR ANALOGUE SOUND-PROGRAMME TRANSMISSION	J.10-J.19
PERFORMANCE CHARACTERISTICS OF ANALOGUE SOUND-PROGRAMME CIRCUITS	J.20-J.29
EQUIPMENT AND LINES USED FOR ANALOGUE SOUND-PROGRAMME CIRCUITS	J.30-J.39
DIGITAL ENCODERS FOR ANALOGUE SOUND-PROGRAMME SIGNALS - PART 1	J.40-J.49
DIGITAL TRANSMISSION OF SOUND-PROGRAMME SIGNALS	J.50-J.59
CIRCUITS FOR ANALOGUE TELEVISION TRANSMISSION	J.60-J.69
ANALOGUE TELEVISION TRANSMISSION OVER METALLIC LINES AND INTERCONNECTION WITH RADIO-RELAY LINKS	J.70-J.79
DIGITAL TRANSMISSION OF TELEVISION SIGNALS	J.80-J.89
ANCILLARY DIGITAL SERVICES FOR TELEVISION TRANSMISSION	J.90-J.99
OPERATIONAL REQUIREMENTS AND METHODS FOR TELEVISION TRANSMISSION	J.100-J.109
INTERACTIVE SYSTEMS FOR DIGITAL TELEVISION DISTRIBUTION (DOCSIS FIRST AND SECOND GENERATIONS)	J.110-J.129
TRANSPORT OF MPEG-2 SIGNALS ON PACKETIZED NETWORKS	J.130-J.139
MEASUREMENT OF THE QUALITY OF SERVICE - PART 1	J.140-J.149
DIGITAL TELEVISION DISTRIBUTION THROUGH LOCAL SUBSCRIBER NETWORKS	J.150-J.159
IPCABLECOM (MGCP-BASED) - PART 1	J.160-J.179
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 1	J.180-J.189
CABLE MODEMS AND HOME NETWORKING	J.190-J.199
APPLICATION FOR INTERACTIVE DIGITAL TELEVISION - PART 1	J.200-J.209
INTERACTIVE SYSTEMS FOR DIGITAL TELEVISION DISTRIBUTION (DOCSIS THIRD TO FIFTH GENERATIONS)	J.210-J.229
MULTI-DEVICE SYSTEMS FOR CABLE TELEVISION	J.230-J.239
MEASUREMENT OF THE QUALITY OF SERVICE - PART 2	J.240-J.249
DIGITAL TELEVISION DISTRIBUTION THROUGH LOCAL SUBSCRIBER NETWORKS	J.250-J.259
IPCABLECOM (MGCP-BASED) - PART 2	J.260-J.279
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 2	J.280-J.289
CABLE SET-TOP BOX	J.290-J.299
APPLICATION FOR INTERACTIVE DIGITAL TELEVISION - PART 2	J.300-J.309
MEASUREMENT OF THE QUALITY OF SERVICE - PART 3	J.340-J.349
IPCABLECOM2 (SIP-BASED) - PART 1	J.360-J.379
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 3	J.380-J.389
MEASUREMENT OF THE QUALITY OF SERVICE - PART 4	J.440-J.449
IPCABLECOM2 (SIP-BASED) - PART 2	J.460-J.479
DIGITAL TRANSMISSION OF TELEVISION SIGNALS - PART 4	J.480-J.489
TRANSPORT OF LARGE SCREEN DIGITAL IMAGERY	J.600-J.699
SECONDARY DISTRIBUTION OF IPTV SERVICES	J.700-J.799
MULTIMEDIA OVER IP IN CABLE	J.800-J.899
TRANSMISSION OF 3-D TV SERVICES	J.900-J.999
CONDITIONAL ACCESS AND PROTECTION	J.1000-J.1099
SWITCHED DIGITAL VIDEO OVER CABLE NETWORKS	J.1100-J.1119
SMART TV OPERATING SYSTEM	J.1200-J.1209
IP VIDEO BROADCAST	J.1210-J.1219
CLOUD-BASED CONVERGED MEDIA SERVICES FOR IP AND BROADCAST CABLE TELEVISION	J.1300-J.1309
TELEVISION TRANSPORT NETWORK AND SYSTEM DEPLOYMENT IN DEVELOPING COUNTRIES	J.1400-J.1409
ARTIFICIAL INTELLIGENCE (AI) ASSISTED CABLE NETWORKS	J.1600-J.1649

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

Supplement 13 to ITU-T J-series Recommendations

ITU-T J.1036 – Factual subscriber-base reporting and protected content delivery in conditional access system – Test methods

Summary

Supplement 13 to ITU-T J-series provides the clause-by-clause test procedures and expected results for each clause of Recommendation ITU-T J.1036 such as log requirements, reports requirements, database requirements, security requirements and more. By applying these test procedures on conditional access system (CAS), two major concerns, 'underreporting of subscribers' and 'content piracy', leading to revenue loss to broadcasters, content providers and the governments', can easily be ascertained.

CAS having sub-standard solutions can be prone to manipulations and vulnerable to hacking, leading to loss of revenue to the concerned broadcasters and the government. Therefore, it is necessary to use tested and certified CAS systems to ensure factual reporting of the subscriber-base and protected delivery of content to authorised subscribers. The purpose of this Supplement is to frame the testing methodology against the various technical requirements of CAS.

In addition to developing a framework for standardization (i.e., technical requirements), some countries have issued provisions for assuring broadcasters and content providers that each CAS system has to conform to certain technical features and get tested by a certified lab before deployment so that piracy and other malpractices can be minimized.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T J Suppl. 13	2023-11-23	9	11.1002/1000/15783

Keywords

Base reporting, conditional access, CAS, piracy, SMS, subscriber management system.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 standards development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 13 to ITU-T J-series Recommendations

ITU-T J.1036 – Factual subscriber-base reporting and protected content delivery in conditional access system – Test methods

1 Scope

This Supplement will provide the clause-by-clause test procedures and expected results for each clause of [ITU-T J.1036] such as log requirements, reports requirements, database (DB) requirements, security requirements and more. By applying these test procedures on CAS, two major concerns, 'underreporting of subscribers' and 'content piracy', leading to revenue loss to broadcasters, content providers and the governments', can easily be ascertained. [ITU-T TR.FSR] provides information on the terminology definition, service scenario, system architecture, and use cases related to [ITU-T J.1036].

2 References

[ITU-T J.1036]	Recommendation ITU-T J.1036 (2023), *Factual subscriber-base reporting and protected content delivery in conditional access system – Requirements*.
[ITU-T TR.FSR]	Technical Report ITU-T TR.FSR, (2023), Technical report on *factual subscriber-base reporting and protected content delivery in conditional access system (CAS).*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 conditional access system (CA) [b-ITU-T J.95]: The complete system for ensuring that cable services are accessible only to those who are entitled to receive them, and that the ordering of such services is not subject to modification or repudiation.

3.1.2 content [b-ITU-R BT.1852-1]: This is any form of digital data that can be acquired and presented by a device.

3.1.3 factual subscriber-base reporting [ITU-T J.1036]: This refers to the accurate and truthful representation of the number of subscribers of each service in a distribution platform without any manipulation or distortion of the underlying data.

3.1.4 piracy [b-ITU-T J.93]: The act of acquiring unauthorized access to programs, usually for the purpose of reselling such access.

3.1.5 protected delivery of content [ITU-T J.1036]: This refers to the secure encrypted transmission of digital content, such as TV programmes, movies, or music, to authorized users while preventing unauthorized access or piracy.

3.1.6 service [b-ITU-R BT.1852-1]: This is one or more data flows intended to be presented together.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CAS	Conditional Access System
DB	Database
FP	Finger Printing
GUI	Graphical User Interface
LCN	Logical Channel Number
OS	Operating Server
SMS	Subscriber Management System
STB	Set Top Box
TEC	Telecommunication Engineering Centre
TRAI	Telecom Regulatory Authority of India
UA	Unique Access
UI	User Interface
VC	Viewing Card

5 Conventions

None.

6 Overview

Conditional access system (CAS) having sub-standard solutions can be prone to manipulations and vulnerable to hacking, leading to loss of revenue to the concerned broadcasters and the government. Therefore, it is necessary to use tested and certified CAS systems to ensure factual reporting of the subscriber-base and protected delivery of content to authorised subscribers. The purpose of this Supplement is to frame the testing methodology against the various technical requirements of CAS.

In addition to developing a framework for standardization (i.e., Technical requirements), some countries have issued provisions for assuring broadcasters and content providers that each CAS system has to conform to certain technical features and get tested by a certified lab before deployment so that piracy and other malpractices can be minimised, see for more information [b-TRAI CP No. 5/2020] telecom regulatory authority of India (TRAI), and the telecommunication engineering centre (TEC) [b-TEC 57015:2022].

7 Test method and expected result

Clause no. in [ITU-T J.1036]	**Test procedure**	**Result expected**
7.1 Log requirements		
[CAS logs] (LOG-REQ 01)	1. Check the commands executed for the following tests – User command – Configuration – Channel/bouquet creation, modification, etc.	1. Logs generated for any change done in configuration related to channel/bouquet creation, modification, deletion, etc. are stored in a secured way.

Clause no. in [ITU-T J.1036]	**Test procedure**	**Result expected**
	in the CAS and try modifying or editing or deleting them, and also altering them. 2. Access the logs of the CAS and check if the logs of such changes are recorded. 3. Check that the logs are in readable format and not editable by any process.	2. Modification / deletion of logs is not allowed. 3. All the CAS logs are exported in readable PDF format only.
(LOG-REQ 02)	Try to change / modify / delete the logs or purge the logs.	Altering or modification of logs is not allowed and there is no facility for the distributor/users to purge the same.
[Time stamping] (LOG-REQ 03)	Commands from the subscriber management system (SMS) are to be sent for the sample set top box(s) (STBs) to the CAS. After sending X number of commands, the audit report / logs from the CAS server are to be taken and the header checked for date, time, and user stamp.	The logs to be checked should match with the commands being sent from the SMS and no mismatch is to be found.
[SMS and CAS integration] (LOG-REQ 04)	Perform all types of activities from the SMS, the same should be reflected in the CAS and the commands should have a date, time, user ID, and unique transaction ID which can be co-related in the SMS and CAS uniquely.	1. All SMS commands pertaining to CAS should be available in transaction logs/report of CAS with date, time and the user / operator stamp. No exception to be found. 2. SMS and CAS are integrated in such a manner that activation and deactivation of the STB happen simultaneously in both the systems.
(LOG-REQ 05)	1. Check that all the transactions being done in the CAS for troubleshooting are being recorded in the logs and there should not be any provision to delete the records. 2. Install / activate the SMS simulator for any troubleshooting purpose. Make one sample client as a test client in CAS. Perform activation / deactivation using operator role user. Extract synchronisation report from CAS.	The extracted report should identify that the commands are sent from CAS for troubleshooting purposes.
(LOG-REQ 06)	Check that all transactions (for any direct operation from the CAS bypassing the SMS) are being recorded in secure logs. Check that the logs history is being maintained for a bare minimum period (say at least the last six months) or prescribed by the concerned regulator from time to time along with the user ID.	Check if the information of these operations carried from CAS directly are properly captured, including user ID. Log records should be maintained as per the time limit prescribed by the concerned regulator.

Clause no. in [ITU-T J.1036]	Test procedure	Result expected
7.2 Report requirements		
(RPT-REQ 01)	Create a few whitelisted cards / STBs in the SMS, activate a few cards or STB, and deactivate a few cards / STBs. Extract active / inactive reports from the CAS graphical user interface (GUI).	CAS reports should be available with active / inactive status with date and time stamp. The action done from the SMS on the targeted card / STBs should be reflected in the CAS status of those cards / STBs and there should be no exception.
(RPT-REQ 02)	Take out the CAS reports of the channel / bouquet subscription and the active / de-active, blacklisted cards, STBs permanently deactivated or killed, and the suspended cards.	Cross-check the reports with the SMS and no exception to be found. The reports should contain the details mentioned in the clause requirement.
(RPT-REQ 03)	Extract the four reports mentioned in the clause requirement from CAS user interface (UI). For card-less STB, in place of a physical viewing card (VC) number, chip-ID or virtual card number may be taken.	1. The reports as per clause requirements should be generated from CAS UI. 2. Cross-check the reports with the SMS and no exception to be found.
7.3 CAS database requirements		
(CDB-REQ 01)	Check the CAS database where data and logs of all activities related to STB activation, deactivation, subscription data, STB unique access (UA) / viewing card (VC) details, entitlement level information, etc., are being stored. Check the list of subscribers.	There shall not be any active unique subscriber outside the database tables.
(CDB-REQ 02)	Run the query on the CAS database to check if there is a way to split the database, or can the database be maintained in multiple servers, run the query through the CAS UI. Check through the CAS server if there are multiple databases or multiple tables. *Note – The testing agency will check through the UI and CAS server if any database split has been enabled. However, by having admin rights, whether the database is split later, may also be checked at an actual deployed site or during regular audits.*	No such way is found to split the data to maintain it on multiple tables / databases / servers by DPO or other.
(CDB-REQ 03)	Understand the process of loading the VC cards or the UA of the STB in the CAS database and whitelist them in CAS. Check whether the information is uploaded by the CAS vendor or the operator. Check the format of the file to see if it can be edited. Check if the	The file cannot be edited and can be uploaded by the CAS vendor only. If the file is uploaded by the operator, then an exception is to be reported and captured in the logs.

Clause no. in [ITU-T J.1036]	Test procedure	Result expected
	uploading of the file is immediately reflected in the CAS database.	
(CDB-REQ 04)	1. Try to gain access to the database through the UI and the manual provided, and check if the database can be modified, deleted, or purged. 2. Check if access to the database is recorded in the logs of the database, i.e., the date and time of accessing the database and by whom. 3. Check access permissions provided to various users on the CAS server. *Note – This may also be checked at the actual deployed site or during regular audits.*	1. Logs of database access should be available. 2. Access should be restricted to the authorised users only and in "read-only" mode only.
(CDB-REQ 05)	Check access permissions provided to various users on the CAS server.	The database audit trail should be permanently enabled.
(CDB-REQ 06)	Export the database details/report from the CAS. Data from SMS may also be pulled.	The CAS database is exported in its entirety to the period and is in a reconcilable format.
(CDB-REQ 07)	Check the database details/report from the CAS with data from the SMS and reconciled without manual intervention.	Reconciliation should be through secure APIs/secure scripts.
(CDB-REQ 08)	Check that CAS and SMS are deployed on separate servers. Self-certification may be obtained.	This may be checked at the actual deployed site or during regular audits.
(CDB-REQ 09)	Check the redundancy architecture or workflow of CAS. All the entries and changes done in the main server are to be cross-checked with the data available in the back server. Switch the backup server to the main server and repeat the process of cross-checking the entries, logs, and reports.	1. The data on the main and backup servers should be in sync. 2. Logs related to main and backup usage are available.
7.4 Security requirements		
[Activation and deactivation] (SEC-REQ 01)	Go through the whole UI through operator ID from the manuals of the CAS vendor and try to carry out the transactions like activating, deactivating, and bouquet creation / modification / deletion of the entries directly from CAS bypassing the SMS.	The CAS UI does not allow any command for activation / deactivation / creation of bouquet or any other activity directly from CAS by bypassing the SMS.
[Logical channel number (LCN)] (SEC-REQ 02)	Feed two channels with the same name or nomenclature through the mux. Check whether the CAS is able to detect the channel with the same name or nomenclature either through their LCN or their service IDs.	CAS should not support the carriage of channels with the same name or nomenclature.

Clause no. in [ITU-T J.1036]	Test procedure	Result expected
(SEC-REQ 03)	Feed two channels with the same name or nomenclature through the mux and check the channels or service IDs created in the SMS and also in the CAS.	CAS and SMS systems should have the same service IDs mapped to each other.
(SEC-REQ 04)	Firewall of the CAS server operating server (OS) may be enabled; or the CAS server may be placed behind an external firewall. Check that access to CAS is restricted through VPN or limited IP addresses and that all other ports are closed.	CAS should be accessible only through firewall.
[CAS server hardware] (SEC-REQ 05)	Check the CAS server: i) OS of server is updated ii) Check password policy - use of strong passwords is enforced iii) No unnecessary third-party software is installed iv) All necessary third-party software are updated v) Anti-virus is activated and updated vi) Firewall access. *Note – The CAS may be deployed on a physical server or cloud server. This clause refers to the capability of CAS to protect against malicious deployments, and cyber security threats. Server hardening may also be checked at the actual deployed site or during regular audits.*	CAS system should be deployed on a secure server.
(SEC-REQ 06)		The CAS server should meet all the requisite security checks.
[Finger printing (FP) measures] (SEC-REQ 07)	1. Send global fingerprinting command from SMS with a minimum of 5 repetitions and random positions. 2. Send unique / individual fingerprinting commands from SMS with a minimum of 5 repetitions and random positions.	CAS should support both covert and visible types of FP functionality. FP should appear on all the targeted STBs each time.
(SEC-REQ 08)		FP should appear on the topmost layer of the video and be visible.
(SEC-REQ 09)		FP should appear each time on all screens of STB in all scenarios mentioned in the clause.
(SEC-REQ 10)		FP should appear each time on all screens and should not be deactivated even if any key on the remote or STB is pressed.
(SEC-REQ 11)		FP should appear as scheduled each time on the boxes and it should change its location on all schedules.
(SEC-REQ 12)		FP should appear each time as per schedule on specific STBs and all STBs.

Clause no. in [ITU-T J.1036]	Test procedure	Result expected
7.5 Service requirements		
[Provision of à-la-carte channels or bouquet] (SER-REQ 01)	Create number of channels on the platform, and check if the same can be created on the CAS and SMS in à-la-carte.	Channel should be able to be created in à-la-carte in both SMS and CAS, and a cross reference report can be generated from CAS and no exception is found.
(SER-REQ 02)	Create some broadcaster bouquets in the CAS and SMS. Also, create some bouquets of the DPO in the CAS and SMS.	Both the CAS and SMS reflect the bouquets created.
[Set top box (STB) operation] (SER-REQ 03)	1. Send commands from SMS for activation of à-la-carte channels, bouquets, and services from the SMS to the targeted STBs. Check at the STBs whether the channels / bouquets get activated or deactivated as intended. 2. Check the status of CAS and SMS logs for each command sent with the date and time stamp.	No exception to be found to the service commands given and the impact seen on the STB.
(SER-REQ 04)	1. Send messages command for payments or payment reminders from SMS to CAS for (i) the active STBs, as well as (ii) the deactivated STBs. The messaging character length should be a minimal 120 characters. 2. Perform the above test for (i) STB switched on, and (ii) STB switched off. 3. STBs to be rebooted to check if the b-mail/ scroll messages are getting displayed in both activated and deactivated conditions.	1. Messages should be displayed on the active as well as deactivated STBs. 2. The messages should be displayed on the active STBs as well as on de-active STBs, both when the STB is "on" and also when the STB is switched "on" from an "off" or "stand-by" state.
[Channel / service addition] (SER-REQ 05)	1. Add a few channels in the SMS through the UI and see if those are encrypted and service IDs created in the CAS. 2. Configure duplicate ECM, AC data, and SID in MUX and check whether CAS is able to detect duplicate ECM/AC/SID data mapped to multiple channels. 3. Check that logs are created in both CAS and SMS in real time for such addition, deletion, and modification of bouquets and à-la-carte services.	1. Additional channels created should reflect both in CAS and SMS and should be able to be activated and deactivated on the targeted STBs. 2. Logs should be created in CAS and SMS in real time for such addition, deletion, and modification of bouquets / à-la-carte services, and such logs are not possible to be altered.
[Hybrid STB] (SER-REQ 06)	Self-certification may be obtained from the distributor of television channels. *Note – This may be checked at the actual deployed site or during regular audits.*	

Clause no. in [ITU-T J.1036]	Test procedure	Result expected
[CAS-STB addressability] (SER-REQ 07)	Report to be generated of the targeted VC / STB in the CAS.	The report should give the current date, time, name of the distributor, and the user ID triggering the report.
(SER-REQ 08)	Report to be generated by VC and by STB number/UA ID of the STB for each channel in the setup, or by bouquet and channels in the bouquet.	Cross-check the reports from SMS, no exception to be found. The channel should be uniquely activated on each STB/UA ID, i.e., if it is in bouquet or à-la-carte, for each VC, it is counted as one.
(SER-REQ 09)	1. Blacklist a few STBs, VCs, UA ID. 2. Send activation command for activating some channels or bouquets for blacklisted STBs and VCs from the SMS.	1. Check if the same STBs/VCs/UA ID are blacklisted in the SMS. 2. Activation on blacklisted VCs and STBs from the SMS should fail.
(SER-REQ 10)	Take an upgradation file for targeting STB's and play it via CAS. Check that the upgrade is received in the targeted STBs. *Note – While the CAS may play the upgradation file, whether the STBs get upgraded or not through OTA would depend on various factors including compatibility.*	CAS should have the required capability.
[De-entitlement of STB] (SER-REQ 11)	Check the status of the VC / STB for the activation periods.	The CAS should comply with either clause, the activation period of the STB/VC in the CAS should be the same as the activation period in the SMS. No exception to being there.
(SER-REQ 12)	Check if the CAS is complying with (SER-REQ 11) above, if not, then it should not have an end date so that it is managed by SMS only.	Either the CAS complies with (SER-REQ 11) above, or it should not have an end date so that it is managed by SMS only.
[Message queue] (SER-REQ 13)	The message should be on a carousel or streamer in the head-end, messages to be created and then played out on scheduled times and repeated after some pre-decided intervals. Check on the sample set of STBs. Repetition of the messages should be checked.	The messages should be queued at the head-end in the event of an unsuccessful transmission.
(SER-REQ 14)		Provision should be available to retry the messages at specified intervals.
(SER-REQ 15)		The life of the messages should be specified for unsuccessful deliveries of messages.
[Geographical blackout] (SER-REQ 16)	Generate different blocks of cards, can be geographical, PIN code based, or other criteria like channels of a particular broadcaster. Configure STBs for different geographical areas. Send commands from SMS to the STBs of the geographical area to be deactivated.	The channels of the targeted STBs should be deactivated.

Bibliography

[b-ITU-T J.93] Recommendation ITU-T J.93 (1998), *Requirements for conditional access in the secondary distribution of digital television on cable television systems*.

[b-ITU-T J.95] Recommendation ITU-T J.95 (1999), *Copy protection of intellectual property for content delivered on cable television systems*.

[b-ITU-R BT.1852-1] Recommendation ITU-R BT.1852-1 (2017), *Conditional-access systems for digital broadcasting*.

[b-TEC 57015:2022] Telecommunication Engineering Centre (TEC), Ministry of Communications, India; (2022), *Test Guide for Conditional Access System (CAS).* <https://tec.gov.in/pdf/TSTP/Test%20Guide%20Final%20CAS%202022_06_15.pdf>

[b-TRAI CP No. 5/2020] Telecom Regulatory Authority of India (TRAI) (2020), *Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services.* <https://www.trai.gov.in/sites/default/files/CP_22042020.pdf>

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

Published in Switzerland
Geneva, 2024