टेस्ट गाइड सं: टीईसी **XXXX:2025**

TEST GUIDE No.: TEC XXXX:2025

इंटरनेट प्रोटोकॉल टेलीविज़न (IPTV) के लिए सब्सक्राइबर मैनेजमेंट सिस्टम (SMS) और कंडीशनल एक्सेस सिस्टम (CAS) के साथ डिजिटल राइट्स मैनेजमेंट (DRM) सिस्टम

Digital Rights Management (DRM) System with Subscriber Management System (SMS) & Conditional Access System (CAS) for INTERNET PROTOCOL TELEVISION (IPTV)

ISO 9001:2015

TELECOMMUNICATION ENGINEERING CENTRE KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Contents

A. History Sheet

S. No.	Test Guide No.	Equipment/ Interface	Remarks
1.	TEC XXXXX:2025	Test Guide for Digital Rights Management (DRM) System with Subscriber Management System (SMS) & Conditional Access System (CAS) for INTERNET PROTOCOL TELEVISION (IPTV)	Month 2025

B. Introduction

Considering the need for developing an overarching framework for standardization, certification and testing of various components of the addressable systems in television broadcasting i.e. Digital Rights Management (DRM) System with Subscriber Management System (SMS) & Conditional Access System (CAS) for INTERNET PROTOCOL TELEVISION (IPTV), Telecom Regulatory Authority of India (TRAI) notified "The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fifth Amendment) Regulations, 2023 (4 of 2023)" on 14.09.2023. These Regulations specify the mandatory as well as the desirable requirements for Digital Rights Management (DRM) System with Subscriber Management System (SMS) & Conditional Access System (CAS) for INTERNET PROTOCOL TELEVISION (IPTV) (Schedule-X); seek compliance by distributors of television channels by deploying such system which conform to these requirements; and ask such distributors to get their DRM systems tested and certified within the stipulated timelines.

TRAI further designated Telecommunication Engineering Centre (TEC) DoT as the Testing and Certification Agency for SMS and DRM used for Broadcasting and Cable TV services as per order dated 14.09.2023.

This Test Guide, prepared as per exhaustive consultations with stakeholders, enumerates detailed test schedule and test procedure for evaluating requirements of Digital Rights Management (DRM) System with Subscriber Management System (SMS) & Conditional Access System (CAS) for INTERNET PROTOCOL TELEVISION (IPTV) as specified in Schedule-X of Telecom Regulatory Authority of India (TRAI) Notification dated 14.09.2023.

C. General Information: (to be filled by testing team)

S. No.	General Information	Details	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of Specifications. against which the approval sought (Schedule-X of TRAI Notification dated 14-09-2023)		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
…			
…			
…			
5	Declaration by Vendor/ Applicant of systems already deployed in India with Name of Distribution Platform Operator (DPOs), Address, Model Number and Serial Number.		
6	Any other relevant Information:-		

D. Testing Team: (to be filled by testing team)

S No.	Name	Designation	Organization	Signature
1.				
2.				
3.				

E. List of the Test Instruments: (to be filled by testing team)

S No.	Name of the test instrument	Make /Model (to be filled by testing team)	Validity of calibration (to be filled by testing team)
1			dd/mm/yyyy
2			
…			
…			
…			
…			

F. Equipment Configuration Offered: (to be filled by testing team) (a)

<Equipment/product name> Configuration:

S No.	Item	Details	Remarks

Relevant information like Software version, Server details, ports, interfaces, size, etc. may be filled as applicable for the product.

(b) <Other equipment name> Configuration:

S No.	Item	Details	Remarks

Relevant information like Software version, Server details, ports, interfaces, size, etc. may be filled as applicable for the product.

G. Equipment/ System Manuals: (to be filled by testing team)

Availability of Maintenance manuals, Installation manual, Repair manual, User Manual etc. **(Y/N)**

H. Test Lab Requirements and General Test Setup:

(a) Test Lab Requirement:

1. Server for the SMS and DRM installation (required only if provider is not providing server).
2. Backup SMS and DRM server*
3. Standard SMS and DRM
4. SMS and DRM Server
5. STBs compatible with the DRM (with fingerprint support, B-mail/ Scroll support)
6. EMM generator
7. ECM Generator
8. Live Channels Streams
9. Multiplexer
10. Up convertors
11. SAS server
12. Networking Switches/ routers
13. Firewall
14. Streamer
15. NTO Document with NCF regulations
16. NDA to be signed by SMS, DRM providers with Test Lab.
17. SMS Server with all the mentioned Interfaces
18. Application (simulated or actual DPO/ LCO Panels) allowing subscribers to choose their channels/ bouquets, etc. (Web interface/ Desktop app/ Mobile app)
19. Any other equipment & test apparatus required for testing of DRM System with SMS & CAS for IPTV.

(b) General Test Setup:

1. Set up IPTV system infrastructure:
   - Configure IPTV streaming server with live/test content.
   - Integrate DRM server with the IPTV headend for encryption of video streams.
   - Ensure the SMS is integrated with the DRM server via secure APIs or control interface.
   - Connect DRM and SMS to the IPTV middleware and subscriber database.
2. Install client-side components:
   - Connect STBs (IPTV capable) to the network and ensure provisioning via SMS and DRM.

- Ensure that each STB is uniquely identifiable via MAC ID or unique subscriber ID.
- DRM-enabled content must stream to whitelisted STBs only.

3. Set up backup DRM server:
   - Include backup DRM server with mirrored configuration.
   - Demonstrate automatic failover and log synchronization between primary and backup servers.
   - Share network diagram reflecting backup infrastructure.
4. SMS user and subscriber provisioning:
   - Create users in SMS with various privilege levels.
   - Create subscriber accounts and assign paired STBs and MAC IDs.
   - Provision bouquets and a-la-carte channels through SMS, reflecting in DRM entitlement.
5. API setup and command flow:
   - List all APIs available between SMS and DRM (e.g., for entitlement, activation, deactivation).
   - Prepare test data and command activity logs to simulate live entitlement changes (activation, deactivation, etc.).
6. Sync and mismatch testing:
   - Input correct data (entitlements and subscriber details) and verify real-time reflection in DRM.
   - Insert incorrect or mismatched subscriber/entitlement data (as per clause 1b(i)–(iv) test criteria).
   - Generate sync and mismatch reports and validate threshold compliance.

I. Clause-wise Test Procedure and Results Expected:

a. DRM Requirements in so far as they relate to subscriber management systems (SMS) for IPTV services (as per Schedule-X notified by TRAI on 14-09-2023)

Clause No	Requirement	Test Procedure	Test Results Expected
1	There shall not be any data mismatch between DRM and SMS. Maximum mismatch based on subscription base may be allowed as mentioned below: (1) Must be less than 0.20% for subscriber base up to 100000 subs (0 to 200 for subscriber base of up to 100000) (2) Must be less than 0.04% for subscriber base up to 1000000 subscribers (0 to 400 for subscriber base of up to 1000000) (3) Must be less than 0.01% for subscriber base above 1000000 subscribers (0 to 1000 for subscriber base of up to 1000000) The data between both the systems shall be reconciled on a monthly basis. The reconciliation report shall be stored along with the system data for a minimum of three (3) years or at least three audit cycles, or as per Schedule III whichever is later.	Extract subscriber data from DRM and SMS for the same date/time. Compare subscriber records (ID, subscription status, packages). Calculate mismatch percentage. Check if mismatch is within the permitted limits based on subscriber base. Verify monthly reconciliation report is stored along with the system data and archival for minimum 3 years or 3 audit cycles.	Mismatch between DRM and SMS is within allowed limit (<0.20%, <0.04%, or <0.01% based on subscriber base). Monthly reconciliation report is generated. Reports are stored for minimum 3 years or 3 audit cycles.

2	**Password Policy Creation for Users:** SMS shall have a defined password policy, with minimum length criteria and composition (upper and lower-case characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof or alternatively user account has to be locked/paired to the Mac Id of the set top box (STB) /unique consumer subscription or the customer premises equipment (CPE)/device.	Password policy to be checked for: -Minimum length criteria -Composition - upper and lower-case characters -Composition - numeric -Composition - alphabets -Composition - special characters -Forced password changes -Attempt to change password of an existing user with and without meeting password policy criteria -Check for alternative mechanism: *Verify whether user account is locked/paired to the MAC ID of the Set Top Box (STB) *Or verify if it is locked/paired to a unique consumer subscription ID *Or verify if it is locked/paired to the Customer Premises Equipment (CPE)/device	The password should meet all the defined password policy requirements. In the absence of a compliant password policy, the system shall enforce user account locking/pairing to the MAC ID of STB / unique consumer subscription / CPE as an alternative security mechanism.
3	**After-Sales Service Support:** The required software and hardware support should be available to the distributor of the television channels' installations from the SMS vendor's support teams located in India. The support should be such as to ensure the SMS system with 99.99% uptime and availability. The systems should have sufficient provisions for backup systems to ensure quality of service and uptime	1. Check if SMS vendor's support teams are located in India. Record details of the local office address, contact details, names of team members, etc. 2. Check the Service agreements and SLAs with the service providers and if they ensure 99.99% uptime. 3. Check uptime for last 3 months/1year.	1. Record details of the support teams located in India. 2. Agreements have provision of required uptime. 3.Uptime availability should be 99.99% or more.

4	All activation and deactivation of STBs/unique consumer subscription shall be done in such a way that SMS and DRM are always integrated and synchronised on real time basis.	Perform activation and deactivation of STBs/unique consumer subscriptions via SMS. Check if the activation/deactivation is reflected immediately in DRM. Verify if SMS and DRM remain integrated and synchronized in real-time during activation/deactivation.	Activation/deactivation in SMS is immediately synchronized with DRM without delay. No mismatch in the subscription status between SMS and DRM after the action.
5	Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscription is reflected in the reports generated from the SMS integrated with the DRM and vice versa	Activate and deactivate STBs/unique consumer subscriptions. Generate reports from SMS and DRM after each action. Check if activation and deactivation events are accurately captured in both SMS and DRM reports.	Activation and deactivation actions are properly recorded and reflected in reports generated from both SMS and DRM.
6	DRM and SMS should be able to activate or deactivate services and/or STBs/unique consumer subscription of the subscriber base of the distributor within 24 hours.	Initiate activation and deactivation requests for services and/or STBs/unique consumer subscriptions via SMS. Monitor the time taken for the actions to be reflected in DRM and SMS systems. Verify completion within 24 hours.	Activation and deactivation requests are successfully completed in SMS and DRM systems within 24 hours.
7	The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately preceding three (3) consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.	Execute various commands (activation, deactivation, etc.) in SMS. Check if logs for each command are generated and recorded.	SMS generates, records, and maintains command logs for at least 3 consecutive years.

		Verify that logs are maintained for a minimum of 3 preceding years.	
8	The SMS should be computerized and capable of recording all logs including information and data concerning the subscribers such as: (a) Unique customer identification (ID) (b) Subscription contract number (c) Name of the subscriber (d) Billing address (e) Installation address (f) Landline telephone number (g) Mobile telephone number (h) E-mail address (i) Channels, bouquets and services subscribed (j) Unique STB number/unique consumer subscription ID attached to a specific unique MAC ID. (k) Unique VC number or MAC ID.	Verify that the SMS system is computerized. Check if SMS records all required subscriber information fields (a) to (k). Review sample subscriber records for completeness and correctness.	SMS is computerized and captures all mandatory subscriber information fields as specified.
9	The SMS should be capable of: (a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs/unique consumer subscription. (b) Locating each and every STB/unique consumer subscription and VC/MAC ID installed at city and state level. (c) Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.	Attempt to view and print historical activation/deactivation data from SMS. Verify ability to locate STB/consumer subscription and VC/MAC ID at city and state levels. Generate and review historical subscription change data, including source of requests.	SMS can view/print activation-deactivation history, locate devices geographically, and generate historical subscription change data with request source.

10	The SMS should be capable of generating reports, at any desired time including about: (a) The total number of registered subscribers. (b) The total number of active subscribers. (c) The total number of temporary suspended subscribers. (d) The total number of deactivated subscribers. (e) List of blacklisted STBs/unique consumer subscription in the system. (f) Channel and bouquet wise monthly subscription report in the prescribed format. (g) The names of the channels forming part of each bouquet. (h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time. (i) The name of a-la carte channel and bouquet subscribed by a subscriber. (j) The ageing report for subscription of a particular channel or bouquet.	Generate reports from SMS for each required parameter (a) to (j). Verify that reports are accurate, up-to-date, and generated at any desired time.	SMS generates all specified reports correctly and on demand.
11	The distributor shall ensure that the SMS vendor has the technical capability in India to maintain the systems on 24×7 basis throughout the year.	1. Verify vendor agreement or contract specifying 24×7 support. 2. Review vendor's support infrastructure in India (e.g., NOC, support centers). 3. Check availability of escalation matrix and support team roster. 4. Interview vendor representatives to confirm readiness and resources for 24×7 support.	1. Vendor agreement explicitly mentions 24×7×365 support. 2. Evidence of a functioning support center/NOC in India. 3. Available escalation matrix and resource availability documented. 4. Confirmation from vendor team on 24×7 support capabilities.
12	DPO shall declare the details of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same shall be notified prior to commissioning of the system, to the broadcasters by the distributor.	1. Verify submitted declarations of DRM and SMS systems to broadcasters. 2. Check records/logs for notifications sent for any additional DRM/SMS deployments. 3. Review timelines of	1. Declaration documents for DRM and SMS are available. 2. Notification records exist for each new DRM/SMS deployment. 3. Notifications were sent before the commissioning dates.

		notifications vs commissioning dates.	
13	If there is active infrastructure sharing (as and when permitted by MIB) then, DPO shall declare the sharing of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same should be notified to the broadcasters by the distributor.	1. Verify whether infrastructure sharing is active and permitted. 2. Review declaration documents regarding shared DRM/SMS. 3. Check records of notifications for any additional DRM/SMS deployments. 4. Confirm timelines of notifications vs commissioning dates.	1. Declaration of shared DRM/SMS is available and submitted. 2. Notification records exist for additional DRM/SMS deployment. 3. Notifications were sent before commissioning of shared systems. 4. Compliance with MIB permission is documented.
14	SMS shall have a provision to generate synchronization report, with date and time, with the minimum fields as listed below: (a) STB/unique consumer subscription Number (or in case of card-less system, chip ID or MAC ID number of the STB) (b) Product Code pertaining to à-la-carte channels and bouquets available on the platform (c) Start Date of entitlement (d) End Date of entitlement (e) Status of STB/unique consumer subscription (active/Inactive)	Activate and deactivate some STBs/ Viewing Cards (VCs) from SMS. Get unsynchronised data; trigger the synchronisation process. Get synchronised data; trigger the synchronisation process.	1. Feature to trigger the synchronisation process is available. 2. This feature generates mismatch reports for both negative (mismatch) and positive (match) cases.
15	The file output of DRM shall be processed by SMS system to compare and generate a 100% match or mismatch error report.	Take DRM data as a CSV/ Excel file. Input this file to SMS and generate a synchronisation report. Test it for both positive and negative scenarios.	1. SMS can process file output of DRM. 2. SMS can generate 100% match or mismatch error report.
16	**Channel/Bouquet management:** SMS shall, in synchronisation with DRM on real time basis, support the following essential requirements:	Create à-la-carte channels, broadcaster's bouquets , platform's own bouquets , their tariffs,	
	(a) Create and manage relevant product ID for all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc.	Create different products with all the given parameters to test. Check the reports in SMS and see	There should be no exception and the reports show all changes with date, time stamp and user id.

		the changes made are reflected or not.	
	(b) Manage changes in the channel/bouquet, as may be required, from time to time.	Make changes in the created bouquets, add/ delete channels from the list. Check the reports in SMS and see the changes made are reflected or not.	There should be no exception and the reports show all changes with date , time stamp and user id.
	(c) Link the Products IDs for à-la-carte channels and bouquets (Single and Bulk) created in DRM with the product information being managed in SMS, for smooth working of SMS and DRM integration.	1. Update the DRM product IDs in the test channels/ bouquets configured for clauses 16(a) and 16(b) above. 2. Use bulk update feature to update Product IDs on all the products.	The reports in SMS should reflect the changes made and there should be no exception. All changes should have date, time stamp and user id.
	(d) Management of historical Data of Product name, i.e., Broadcasters (name), maximum retail price (MRP), distributor retail price (DRP).	Modify the details on different dates for same product. Include the TRAI NTO.x regulation of per channel rate and bouquet rate and content rate. Check each case with all combinations. Check the historical changes done on all the parameters like channels, pricing, bouquet, DRP, MRP.	The report should give the chorological changes done , with time and date stamp and user signatures at the time of changes.

17	**Network Capacity Fee (NCF) Policy Creation:** SMS shall support all NCF related requirements mandated by the applicable tariff order.	1. Check the availability of the NCF parameters. 2. Add and delete a few channels in the NCF package, check the price change. 3. Check its implementation in Subscriber Billing. 4. Take Point of all the validations related to NCF calculation from TRAI NTO.x regulations. Check each point.	1. Feature to manage NCF Policies with all its parameters is available. 2. The reports on NCF are as desired with all the parameters (the number of TV channels, name and the prices). 3. Resultant Billing Reports are as expected.
18	**Bill/Invoice Generation:** SMS shall be capable of generating proper subscriber bill/invoice with explicit details of NCF charges, pay channels charges (with clear itemized details of à la-carte channel cost and bouquet costs), rental charges for STB/unique consumer subscription (if any), other applicable charges, including Goods and Services Tax (GST).	Check previously raised invoices. Check if the billing is on per day basis. Generate invoices for the targeted subscribers for Prepaid, Post-paid and Advanced Paid Subscriptions. Also generate invoices with and without taxes, invoices with and without NCF. Check each component mentioned in the clause requirement.	SMS should generate proper subscriber bill/ invoice with explicit details as per clause requirements such as NCF fee, pay channel charges, itemised billing for the pay channels à-la carte and bouquet, GST and any other charges. The invoice should show the start date and end date and the same should tally with the subscriber entitlement dates on the cards and end date in the SMS.
19	**Management of Logs:**		
	(a) SMS shall have the facility to provide user detail logs with the ID of users on each login event.	1. Keep a note of all the logins and logouts done by various users. 2. Fetch the Login Logout Report and verify it	1. Verification should match 100%. 2. The logs cannot be deleted or modified.

		with the information noted.	
	(b) SMS shall have the provision of generating the user activity log report to enable tracking users' work history. It shall not be allowed to delete the records from the log.	1. Keep a note of all the Activities done on SMS. 2. Fetch the Log Report and verify it with the information noted. 3. Scan the whole SMS for the feature of editing the logs.	1. The reports should be able to give the user working history and changes done. 2. The logs cannot be deleted or modified.
	(c) All logs shall be stamped with date and time and the system shall not allow altering or modifying any logs.	Access logs of the SMS and check that the logs are not editable by any process.	1. All log reports should have time stamp, date stamp and user id with it. 2. There is no feature to modify, alter or delete the logs. 3. All the logs are exported in readable and un-editable format.
	(d) The logs shall be maintained for a period as specified in Schedule III or at least three audit cycles, whichever is later.	1. Check the history of logs maintained in the SMS and check if they meet the requirement of Schedule III. 2. Take out random reports of the logs and verify the date, timestamp, user-id login. 3. Check if there is an option of auto delete. Change the SMS Server dates and perform activities and then verify if the data is	1. Logs are as per schedule III. 2. Logs contain Date & Time Stamp with User-ID. 3. No way to modify the logs. 4. Delete or purge option, if any, is only for the logs older than 3 years or as described in Schedule III.

		auto deleted of 3 years of period.	
	(e) Channel subscription report: SMS shall be able to provide broadcaster wise total counts of monthly subscribers of channels including both à la carte and bouquet subscriptions as per format that may be prescribed by TRAI.	1. Add and Modify the Subscription data and keep a note of all the modifications. 2. Fetch the reports (all combinations of à-la-carte, bouquet both of broadcaster and DPO) 3.Verify that the report provides broadcaster-wise subscriber counts. 4.Ensure the report is generated in the format prescribed by TRAI, if specified. 5. Compare the data in the SMS report with CAS data for accuracy and consistency. with the CAS data.	SMS should generate the broadcaster-wise channel subscription report. The format of the report should comply with TRAI-prescribed format (if provided). There should be no variance during comparison with CAS data.
	(f) DRM and SMS should be running on separate and independent servers.	1. Review network architecture diagrams showing server setup. 2. Physically or remotely verify that DRM and SMS are hosted on different servers. 3. Check system configuration and server details to confirm independence (no shared hardware or VM).	1. Architecture diagrams clearly show separate servers for DRM and SMS. 2. Independent server hosting is verified. 3. No shared resources between DRM and SMS systems.
20	**SMS Database and tables:**		

	(a) There shall not be any active unique subscriber outside the database tables declared by the Vendor	Check the database, does it exist on one server or multiple servers, does it has a backup server, how frequently data is synchronised between backup and main, is data stored in cloud; generate random reports of the active subscribers, de-active subscribers, blacklisted cards/ STB.	Check the random reports and there should not be any exception of any VC or STB missing in any data report of active/ deactivate subs, blacklisted cards or whitelisted cards. SMS should include all active STB/ VC numbers irrespective of their status i.e. suspended, in stock/ testing/ repairable/ non repairable.
	(b) SMS shall not provide an option to split SMS database or for creation of more than one instance.	Run the query on the SMS database to check if there is way to split the database, or can the database be maintained in multiple servers, run the query through the SMS UI. Check through the SMS server if there are multiple databases or multiple tables. Note: The testing agency will check through the UI and SMS server if any database split has been enabled. However by having admin rights, whether the database is split later, may also be checked at actual deployed site or	No such way is found to split the data to maintain it on the multiple tables/ databases/ servers.

		during regular audits.	
	(c) SMS shall have the provision to enable or disable channel (à-la-carte channel or bouquet of channels) selection by subscribers either through website or an application through interface provided by the distributor platform operator.	1. Check if the SMS is capable of accepting inputs through the interface of the application (simulated or actual DPO/ LCO Panels) allowing subscribers to choose their channels/ bouquets, etc. (Web interface/ Desktop app/ Mobile app). 2. Login as a subscriber in the application and select à la-carte channels and bouquets. Check if the selections are reflected in the SMS.	1. The SMS should have provision to interface with the DPO/ LCO application/ web interface. 2. The changes done as subscriber from all the three modes, web interface, desktop app and mobile app should reflect in the SMS and also be in DRM and should be done instantaneously. If any delay, the same should be noted along with the exception.
	(d) SMS shall be capable of capturing the following information required for audit or otherwise: i. Bouquet à la carte status change history ii. Bouquet composition change history iii. Change in status of connection (primary to secondary and vice versa)	1. Make changes in test channels à-la-carte and Bouquet composition configured for clause 16(a) above. 2. Designate a set of STB as primary and few secondary, then change the sequence in the same STB. 3. Check the history reports maintained in the SMS for all the changes done as required for clauses 20d(i) to 20d(iii).	No historical data is missing in the history reports.

21	SMS shall be accessed through a Firewall	Firewall of the SMS server OS may be enabled; or, SMS server may be placed behind external firewall. Check that access to SMS is restricted through VPN or a limited IP addresses and all other ports are closed. Note: The DPO might use the firewall of the SMS server OS or a perimeter firewall. Restricted access to SMS through firewall may also be checked at actual deployed site or during regular audits.	SMS should be accessible only through Firewall.
22	STB/unique consumer subscription and MAC ID shall be paired from the SMS to ensure security of channel (applicable for DRM with pairing facility).	1.Verify pairing mechanism in SMS: -Ensure SMS supports pairing of STB with MAC ID or unique consumer subscription ID. 2. Initiate pairing of a channel subscription to a specific STB/MAC ID or consumer subscription. 3. Attempt to access the channel from: -The paired device (should succeed). -An unpaired device (should fail). 4. Check logs/records in SMS confirming the pairing enforcement. 5. If applicable, verify DRM integration to ensure pairing enforcement is active.	1. SMS should successfully enforce pairing of STB/unique consumer subscription and MAC ID for subscribed channels. 2. Channel access should only be allowed through the paired device, thereby ensuring content security as per DRM requirement.

23	The SMS shall be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB/unique consumer subscription by STB/unique consumer subscription basis.	Take the report of a few subscribers, it should be triggered with parameters like channel reports, STB reports i.e. details of channels active on the targeted STBs, and also details of STBs active for the targeted channels. Compare with the reports from DRM.	The SMS should generate channel-wise and STB-wise reports. These reports should tally with the reports from DRM.
24	SMS should have a facility to carry out monthly reconciliations of channels/a-la-carte and bouquet (with their respective ID created in SMS with DRM) and the variance report should be available from the DRM and SMS logs and made available during audits.	1. Trigger monthly Reconciliation Option in SMS. 2. Do some direct entries in DRM to create a mismatch in SMS and DRM. 3. Check Reports for both Match and Mismatch of Data.	SMS should generate correct Mismatch and Match Reports.
25	SMS should have a provision of generating the following reports pertaining to STB/unique consumer subscription/MAC ID.:	1. Check the availability of each report for clauses from 25(a) to 25(g) 2. Prepare data for each report. 3. Generate each report and reconcile with DRM for clauses 25a, 25b, 25d, 25e, 25f and 25g. For the point 25c, reconcile with the stock ledger of store.	Feature available and generating reports for clauses from 25(a) to 25(g) as expected.
	(a) White list of STB/unique consumer subscription /MAC ID along with active/inactive status		
	(b) Faulty STB/unique consumer subscription/MAC ID – repairable and beyond repairable		
	(c) Warehouse fresh stock		
	(d) In stock at local cable operator (LCO) end		
	(e) Blacklist		
	(f) Deployed with activation status		

	(g) Testing/demonstration STB/unique 1 consumer subscription /MAC ID with location		
26	**Audit-related requirements:** SMS should have the capability to capture below-mentioned information that may be required for audit and otherwise:		Resultant report is as desired. For 26(a) to 26(c).
	(a) Subscriber related:		
	(i) Subscriber contact details change history	1. Change the contact details of a subscriber on different dates. 2. Check the effect in the Subscriber Contact Details History Report.	
	(ii) Connection count history	1. Create and activate and deactivate some subscribers on different dates. 2. Check the connection count report is effected or is it showing only the current count. 3. If MSO has implemented multiple DRM, extract the report for each DRM date-wise.	
	(iii) Transition of connection between Disconnected/Active/Temporary Disconnected	1. Move the connection of one subscriber from one state to another (Active/ Temporary Disconnected/ Disconnected). 2. Check the report for its history with date.	
	(iv) Subscription change history	1. Change the subscription of Bouquet and à-la-carte of one connection on different dates. 2. Check the report	

		which shows subscription history of the connection.	
	(b) Product (Bouquet/à-la-carte channel) related:		
	(i) Broadcaster à-la-carte relation	1. Change Broadcaster à-la carte data on different dates. 2. Check the report that shows the change history of the data.	
	(ii) Bouquet name change history	1. Change bouquet name data on different dates. 2. Check the report that shows the change history of the data.	
	(iii) À la carte name change history	1. Change à-la-carte name data on different dates. 2. Check the report that shows the change history of the data.	
	(iv) Bouquet/à-la-carte channel rate change history	1. Change bouquet à-la-carte channel rate data on different dates. Also check on renewal and subscription screens. 2. Check the report that shows the change history of the data.	
	(c) STB/unique consumer subscription related:		
	(i) Change in location history	1. Change location of a STB/ subscriber on different dates. 2. Check the report that shows the change history of the data.	

	(ii) Change in status (Active/Damaged/Repaired/Replaced)	1. Change status of a STB/ subscriber on different dates. 2. Check the report that shows the change history of the data.	
27	**User Authentication:** SMS should have the capability to authenticate its subscribers through registered mobile number (RMN) through one-time password (OTP) system	Check that the SMS generates OTP during following activities: 1. Registration of Mobile number 2. Connection activation 3. Subscription Change Completion of these activities will depend on the OTP verification.	1. SMS generates OTP. 2. Activities mentioned in test procedure completed successfully with OTP and failed without OTP verification.
28	SMS should have the provision to support the following additional requirements:		
	(a) List of à-la-carte channels and bouquets, digital headend (DHE): Provision to support/ Sub-Headend-wise list of à-la-carte channels and bouquets, in sync with the list available in DRM.	1. Create digital headend (DHE) and Zone. 2. Mark the products that need to be visible under a specific DHE/ Zone. 3. Check if the products are available for use as per their respective DHE/ zone.	1. Functionality is available. 2. The filter is working as expected.

	(b) Product (à-la-carte channels and bouquets)-wise Renewal and Reversal setting for the Subscriber Account: Provision to allow renewal of a product to a subscriber after the expiry date of a product, and provision to auto-calculate and refund the amount to a subscriber if he discontinues a product midterm. These requirements may be configurable on selective products, as required by the DPOs as per their business plans.	1. Mark a product A to be Auto-Renewable. 2. Mark a product C to be Manually-Renewable. 3. Mark a product B to be Refundable on a pro-rata basis. 4. Mark a product D to be non refundable. 5. Subscribe to products A and B on some connections. 6. Wait for the expiry date of products A and C. 7. Discontinue products B and D on any one of the connections before their expiry date.	1. Product A will be auto renewed for the next cycle. 2. Product C will be unsubscribed. 3. There will be a refund entry for Product B based on the remaining days of expiry. 4. No refund will be there for product D.
	(c) Product (à-la-carte channels and bouquets)-wise Reversal setting for LCO Account: Provision to calculate and refund the amount due to LCO, if he or the subscriber discontinues a product midterm. Product (à-la-carte channels and bouquets) Tenurewise LCO and Subscriber Discount Scheme/Free Days Scheme: Provision to create Discount Scheme and Free-day scheme for LCO and Subscriber, based on the duration (Tenure) of the product subscription.	1. Create Discount Policies based on Tenure for LCO. 2. Create Discount Policies based on Tenure for Subscriber. 3. Give subscriptions on one of the connection.	Subscriptions discount days should get added automatically.
	(d) Calendar/Activity Scheduling: Provision to auto-schedule activities like STB/unique consumer subscription activation/deactivation, à-la-carte channels and bouquets addition/removal, channel/bouquet composition modification, etc.	Check the provision to auto schedule activities for future executions of: 1. Connection activation/ deactivation 2. à-la-carte channels and bouquets addition/ removal 3. channel/ bouquet composition modification	1. Provision is available. 2. The scheduled activity got executed successfully on the given date.

	(e) Bulk Channel/Bouquet Management: Provision to perform bulk activity of à-la-carte channels and bouquets addition and removal on all or a designated group of STBs/unique consumer subscription.	1. Select all or a group of active STBs/unique consumer subscription. 2. Select a channel and/ or a bouquet to add it to all the above selected STBs/ unique consumer subscription. 3. Add the product as a bulk operation. 4. Similarly, select a channel and/ or a bouquet to remove it from all the above selected STBs/ unique consumer subscription. 5. Remove the product as a bulk operation.	1. In addition to the process of selecting one STB/ unique consumer subscription at a time and add or remove the product, the feature of bulk operation is available. 2. The result of the feature is as expected.
	(f) Token-number-based reports: Provision to download multiple generated reports with the help of token number, such as audit reports with different intervals.	1. Generate the report. 2. The report process gives a token number and goes in the background*. 3. Go to the centralized screen to check the status of the generated report. Download the report. *Check if the feature of background worker for Reports is available. There may be different ways to implement it. One of the implementation logic can be that the report is generated and uploaded to a centralized	1. Feature of downloading multiple generated reports with the help of token number is available. 2. The result of the feature is as expected.

		location and can be downloaded from there later. Its importance is when we have big data for a report e.g. audit reports.	
	(g) Third-Party Integration: Provision to support integration with relevant third-party systems, such as, payment gateway integrations, interactive voice response (IVR) Integrations, SMS Gateway Integrations, etc.	Check whether the SMS has been integrated with: (i) payment gateway (ii) interactive voice response (IVR) (iii) SMS Gateway (iv) email Gateway (v) any other third-party systems.	Record the details of third-party systems with which the SMS has been integrated.
	(h) Bill payment and reconciliation feature: Provision for bill payment and reconciliation (in case a DPO is running service in post-paid mode).	Generate bills for various STBs. Enter payment details for a few STBs. Generate reports for outstanding bills and paid bills.	Verification of reports done successfully.
	(i) Generation of Reports: Provision to generate the following reports for operational purpose:	1. Prepare fresh data concerning the report to be tested for each of the clause from 28l(i) to 28l(iv). 2. Extract the corresponding report and verify it with the activity done and data prepared.	Verification of reports done successfully for clauses from 28l(i) to 28l(iv).
	(i) All, selective and single boxes' current status with their first-time activation date.		
	(ii) Total number of à-la-carte channels and bouquets and STB/unique consumer subscription expiring detail till given future date on the dashboard, according to the permission.		
	(iii) Today's fresh activation count, de-activation count, re-activation count, à-lacarte channels and bouquets addition/ removal count on dashboard, according to the permission.		

	(iv) Total active and inactive subscriber's details with multiple criteria (network-wise, à-la-carte channels and bouquets-wise, state city wise and broadcaster-wise).		
29	It shall be mandatory for SMS to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers, in an automated manner without any manual intervention. Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server: Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc.	1. Verify the existence of a backup server for SMS. 2. Review system configuration for automated backup without manual intervention. 3. Check logs to confirm concurrent copying of activities. 4. Review records of any switchover events from backup to main server, along with date/time stamps. 5. Verify data synchronization between main and backup servers (subscription data, STB UA/MAC ID, entitlements, etc.).	1. Backup server is available and operational. 2. Automated concurrent backup process is configured and working. 3. Logs confirm continuous copying without manual input. 4. Switchover logs are properly maintained with timestamps. 5. Main and backup servers are fully synchronized for all critical data.

B. DRM Requirements for conditional access by subscribers and encryption for IPTV services (as per Schedule-X notified by TRAI on 14-09-2023)

Clause No	Requirement	Test Procedure	Test Results Expected
1	DPO shall ensure that the current version of the DRM in use do not have any history of hacking. A written declaration from the DRM vendor shall be required to be furnished on an annual basis as compliance of this requirement.	1. Obtain and review the written declaration from the DRM vendor confirming no hacking history. 2. Verify that the declaration is updated annually. 3. Cross-verify available security advisories and public vulnerability databases for any reported incidents.	1. Annual declaration from DRM vendor available and up-to-date. 2. No known hacking history associated with the deployed DRM version. 3. No critical vulnerabilities reported.

2	DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all activations, deactivation, channel authorization/assignment and un-authorization / de-assignments and change in MAC ID/STB/unique consumer subscription). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs.	1. Perform multiple transactions via DRM such as: -Activation and deactivation of services -Channel authorization and un-authorization -Assignment and de-assignment of channels -Change of MAC ID/STB/unique consumer subscription 2. Retrieve the logs from the DRM system and verify each entry has proper date, time, and transaction details. 3. Attempt to modify, delete, or purge any log entries through the user interface or backend (if accessible). 4. Confirm that log immutability is enforced by the system and no alterations are possible.	All logs in the DRM are accurately time-stamped and include details of all relevant transactions (activations, deactivations, channel changes, MAC ID/STB/consumer ID updates). Logs are immutable — they cannot be modified or deleted by any user. There is no provision for log purging by distributors or users.
3	DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) /unique consumer subscription directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs/unique consumer subscription shall be done with the commands of the SMS (provided that such feature may be available only for specific testing. The command or access for such feature may be available with the highest system administration password. In all such cases a separate log file of such commands has to be maintained) integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel.	1.Review the DRM GUI: -Attempt to locate any interface that allows direct activation/deactivation of STB or unique consumer subscription. 2. Try to activate/deactivate a test client directly via DRM GUI using operator-level credentials (should not be permitted). 3. If any such action is available under highest-level admin credentials: -Attempt the activation/deactivation under supervision. -Verify whether a separate log file of this action is automatically created and includes: Date/time Command executed User ID used Device/subscriber details affected 4. Confirm that all routine	1. No direct activation/deactivation is permitted from the DRM GUI under operator or general access roles. 2. Any admin-level operation, if performed, is: -Securely logged in a separate log file -Includes complete traceability (timestamp, user ID, action, device info) -Retained for at least six months 3. All regular operations are routed through SMS commands, ensuring DRM-SMS integration for secure channel access. 4. Channel security remains intact, with no bypass of SMS permitted in operational flow.

		activation/deactivation activities are only possible via SMS-integrated commands. 5. Extract reports/logs from DRM and check whether unauthorized or direct operations are prevented or properly logged. 6. Verify that six-month history of any direct command (if applicable) is retained and retrievable.	
4	The SMS and the DRM should be integrated in such manner that activation and deactivation of STB/unique consumer subscription happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscriptions is reflected in the reports generated from the DRM.	1. Activate and deactivate multiple STBs/unique consumer subscriptions using the SMS interface. 2. Immediately fetch transaction logs/reports from both SMS and DRM systems. 3. Compare records for each transaction (activation and deactivation) in both systems to verify synchronization. 4. Attempt controlled scenarios (e.g., network delay or partial command loss) to verify whether the DRM still reflects accurate final states. 5. Verify whether every transaction initiated via SMS is fully captured and mirrored in DRM reports with: Timestamp Subscriber ID Device/STB/MAC ID Transaction type (activation/deactivation) 6. Check if there is any mismatch or time lag in reflecting these transactions in DRM.	Every activation and deactivation command initiated via SMS is reflected in DRM system and visible in its transaction reports. Reports from SMS and DRM show complete synchronization for all transactions. No mismatch or inconsistency is observed between SMS and DRM logs for activation/deactivation. The integration ensures simultaneous reflection of actions across both systems, satisfying the requirement.

5	DRM deployed should be able to support two-way networks only.	1. Review DRM system specifications and technical documents. 2. Check system design to ensure support for two-way communication (downlink and uplink channels). 3. Verify through test reports or live system demo that two-way communication is functional.	1. DRM system specifications confirm two-way network support. 2. System design shows bidirectional communication capability. 3. Test reports or demos validate two-way network operation.
6	The DRM deployed should be able to support both carded as well as card-less STBs/unique consumer subscription for any provisioning.	1. Review DRM system specifications for support of carded and card-less STBs/unique subscriptions. 2. Verify provisioning workflows for both carded and card-less devices. 3. Test the activation and authorization process for a sample carded and card-less STB/consumer device.	1. DRM documentation confirms support for both carded and card-less devices. 2. Provisioning process is functional for both device types. 3. Successful activation and authorization observed for carded and card-less STBs/subscriptions.

7	The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last three (3) years minimum. The reports must have date and time stamp. Proposed reports should include: (a) Unique active STB/unique consumer subscription count as well as MAC ID wise on any desirable date (b) Unique bouquet/channel active for a specific STB/unique consumer subscription on any desirable date (c) MAC ID/User ID wise activation-deactivation report for service requests (d) Any alteration in bouquet and/or channels configured in DRM (e) Blacklist STB/unique consumer subscription report (desirable not mandatory feature) (f) Product code pertaining to channels/ bouquets available on the platform (g) Channel/bouquet authorization/assignment to STB/unique consumer subscription along with start date and end date of entitlement (h) STB/unique consumer subscription -VC pairing / de-pairing or User id-Mac-id Pairing / de-pairing (if applicable) in SMS/DRM (i) STB/unique consumer	The DRM deployed should be able to generate, record, maintain independent reports and logs for verification during audits for at least 3 years, with date and time stamps, covering specific report types (a) to (u).	1. Review DRM system capabilities for report generation and log maintenance for 3 years minimum. 2. Verify that reports include date and time stamps. 3. Check sample reports for all specified report types (a) to (u). 4. Verify archival and retrieval process for historical data. 5. Confirm that no manual intervention is required for logging activities.

	subscription activation / de-activation (j) Channels assignment to STB/unique consumer subscription (k) Report of the activations or the deactivations of a particular channel for a given period (l) The total number of registered subscribers (m) The total number of active subscribers (n) The total number of temporary suspended subscribers (o) The total number of deactivated subscribers (p) List of blacklisted STBs/unique consumer subscription in the DRM (desirable not mandatory feature) (q) Channel and bouquet wise monthly subscription report in the prescribed format. (r) The names of the channels forming part of each bouquet (s) The total number of active subscribers subscribing to a particular channel or bouquet at a given time (t) The name of a-la carte channel and bouquet subscribed by a subscriber (u) The ageing report for subscription of a particular channel or bouquet		

8	DRM deployed should be able to tag and blacklist the STB/unique consumer subscription in case of any piracy.	1. Simulate or mark a few STBs or unique consumer subscriptions as involved in piracy within the DRM system. 2. Tag and blacklist the marked STBs/consumer subscriptions using the DRM's blacklisting feature. 3. Attempt to send activation or channel assignment commands for these blacklisted entries via SMS. 4. Attempt to access services from the blacklisted devices/subscriptions. 5. Check whether these blacklisted entries are also reflected in SMS (if synchronized) or denied at DRM enforcement level.	1. The blacklisted STBs/unique consumer subscriptions are successfully tagged in DRM, and corresponding access is blocked. 2. Activation or channel assignment commands sent from SMS for blacklisted devices/subscriptions fail at DRM level. 3. Blacklisted entries are not able to access any service, ensuring piracy control. 4. The DRM system ensures irreversible enforcement of blacklisting, preventing re-use or redeployment.
9	DRM deployed should have the technical capability in India to maintain the systems on 24x7 basis throughout the year.	1. Verify vendor agreements or SLAs mentioning 24×7 support. 2. Review the support infrastructure and team availability in India. 3. Check escalation matrix, contact points, and shift schedules. 4. Interview DRM vendor representatives regarding 24×7 readiness.	1. SLA/vendor agreement confirms 24×7×365 support. 2. Support center and technical resources are operational in India. 3. Escalation and contact details are properly documented. 4. Confirmation of 24×7 system maintenance capability.

10	The DRM and SMS should be integrated in such manner that upon deactivation of any subscriber from the SMS, all program/services shall be denied to that subscriber.	1.Use the SMS to deactivate a subscriber (STB/unique consumer subscription). 2.Attempt to access all types of content (FTA, pay channels, and platform services) on the deactivated subscriber's STB. 3.Verify logs from both SMS and DRM to ensure that the deactivation command was transmitted and executed with: Accurate timestamp Device/subscriber details Service block details 4.Confirm denial of access through actual STB output (no content playback). 5.Repeat the test for multiple subscriber profiles and services to ensure consistent behavior.	On deactivation via SMS, all services are denied to the subscriber through DRM enforcement. DRM and SMS logs reflect correct and synchronized command execution with appropriate timestamps. No exception or residual access is observed on the STB after deactivation. The integration ensures complete and effective denial of service upon SMS deactivation.
11	The DRM should be capable of generating, recording and preserving unedited data / logs for at least three consecutive years for each command executed through the DRM, including logs of each command of the SMS integrated with the DRM.	1. Review DRM system specifications and logging policy. 2. Verify the log retention settings and storage capacity for at least three years. 3. Check samples of historical logs for completeness and integrity (unedited records). 4. Confirm logs capture both DRM and integrated SMS command activities.	1. DRM system generates and preserves unedited logs for minimum three years. 2. Log samples are complete, accurate, and cover all command executions. 3. Logs from both DRM and SMS commands are maintained. 4. No manual alteration possible in the logs.

12	DRM deployed should be capable to support both software base as well as hardware base security.	1. Review DRM system technical specifications for security support. 2. Verify support for software-based security (e.g., device-based encryption, app-level protection). 3. Verify support for hardware-based security (e.g., Trusted Execution Environment (TEE), Secure Chip). 4. Check system demonstration or documentation validating both security modes.	1. DRM system supports software-based and hardware-based security mechanisms. 2. Technical documents confirm both methods are available. 3. System demonstration (or logs) verifies functioning of both security types.
13	DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS.	1. Add few channels in the SMS through the UI and see if those are encrypted and service ids created in the DRM. 2. Configure duplicate ECM, AC data and SID in MUX and check whether DRM is able to detect duplicate ECM/AC/SID data mapped to multiple channels. 3. Check that logs are created in both DRM and SMS in real time for such addition, deletion, modification of bouquets and à-la-carte services.	1. Additional channels created should reflect both in DRM and SMS and should be able to be activated, deactivated on the targeted STBs. 2. Logs should get created in DRM and SMS in real time for such addition, deletion, modification of bouquets / à-la-carte services and such logs are not possible to be altered.
14	DRM should be so configured for specific type of STB/unique consumer subscription, that are procured and configured by the DPO. The DRM should not enable working/operation of any other type/brand/make of STB/unique consumer subscription, in the network.	1. Review DRM configuration settings for STB/device whitelisting. 2. Verify approved list of STBs/consumer devices provided by DPO. 3. Attempt connection/activation of an unauthorized STB/device and observe system behavior. 4. Review system logs for	1. DRM is configured to allow only DPO-approved STBs/devices. 2. Unauthorized STBs/devices fail to connect or operate. 3. System correctly logs attempts by unauthorized devices. 4. No unauthorized device is functional on the network.

		unauthorized device rejection events.	
15	When infrastructure sharing (as and when permitted by MIB) is available, in such cases DRM shall be capable to support multiple DPOs.	1. Review DRM system architecture and design documents. 2. Verify configuration options for multi-DPO support. 3. Check test cases or demos showing multiple DPO profiles or partitions within the DRM. 4. Confirm proper segregation of data and entitlements across DPOs.	1. DRM system is capable of handling multiple DPOs simultaneously. 2. Each DPO's data and entitlements are securely segregated. 3. Test/demo confirms DRM operations for multiple DPO environments without conflict.
16	DRM should support content protection.	1. Review DRM system specifications for content encryption and protection features. 2. Verify encryption standards (e.g., AES, Widevine, PlayReady) implemented. 3. Check live system or demo to confirm encrypted delivery of content. 4. Review security certifications or audit reports (if available).	1. DRM system supports recognized content protection mechanisms. 2. Content is encrypted during transmission and storage. 3. Demo or system validation confirms protected content delivery. 4. Security documentation supports compliance with content protection standards.
17	DRM should support key rotation, i.e., periodic changing of security keys	1. Review DRM system documentation for key rotation feature. 2. Verify configuration settings for key rotation intervals and policies. 3. Check sample logs or audit trails showing historical key changes. 4. Observe or request a demonstration of the key rotation process.	1. DRM system supports automatic or configurable key rotation. 2. Key rotation is performed at defined intervals without service interruption. 3. Logs/audit trails confirm periodic key changes. 4. Content remains protected throughout key changes.
18	In case DPO has deployed hybrid STBs (hybrid STB for the purpose of this regulation means a STB that uses multiple methods of receiving transmission signals with video and audio content, however in a single	Self-certification may be obtained. Note: This may be checked at actual deployed site or during regular audits.	

	instance such STB provides only one type of service), DRM shall ensure that the over the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.		
19	There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor.	Run the query on the DRM database to check if there is way to split the database, or can the database be maintained in multiple servers, run the query through the DRM UI. Check through the DRM server if there are multiple databases or multiple tables. Note: The testing agency will check through the UI and DRM server if any database split has been enabled. However by having admin rights, whether the database is split later, may also be checked at actual deployed site or during regular audits.	No such way is found to split the data to maintain it on the multiple tables/ databases/ servers.

20	It must support the following options with reference to uploading of unique access (UA)/MAC ID details in DRM database: (a) A secure un-editable file of MAC ID details, as purchased by the distributor, to be uploaded by the DRM vendor on the DRM server directly, (b) If it is uploaded in any other form, UA/MAC ID in DRM database shall be captured in logs,	Understand the process of loading the MAC ID or the UA of the STB in the DRM database, whitelist them in DRM. Check whether the information is uploaded by the DRM vendor or the operator. Check the format of the file to see if it can be edited. Check if the uploading of the file is immediately reflected in the DRM database.	The file cannot be edited and can be uploaded by the DRM vendor only. If the file is uploaded by the operator then an exception to be reported and captured in logs.
	(c) Further, DRM shall support an automated, application programming interface (API) based mechanism to populate such UA/MAC ID details in the SMS, without any manual intervention.	Upload a file of the MAC ID details/ UA IDs of the STB in the DRM, try blacklisting some MAC ID details in DRM.	The same MAC ID details/ UA ids of the STB should be reflected in SMS; the same MAC ID details should be blacklisted in SMS and no activation or deactivation on those cards can be done.
21	It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers: Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server: Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc	Check redundancy architecture or workflow of DRM. All the entries and changes done in the main server to be cross checked with the data available in the back server. Switch the backup server to main server and repeat the process of cross-checking the entries, logs, reports.	1. The data on main and backup servers should be in sync. 2. Logs related to main and backup usage are available.

22	DRM and SMS shall ensure that the access to database is available to authorized users only, and in "read only" mode only. Further, the database audit trail shall be permanently enabled. Explanation: Database here refers to the database where data and log of all activities related to STB/unique consumer subscription activation, deactivation, subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc., is being stored.	1. Try to gain access to the data base through the UI and manual provided, check if the database can be modified, deleted or purged. 2. Check if the access to data base is recorded in the logs of the data base, i.e. date and time of accessing the database and by whom. 3. Check access permissions provided to various users on the on DRM server. Note: This may also be checked at actual deployed site or during regular audits.	1. Logs of database access should be available. 2. Access should be restricted to authorised users only and in "read only" mode only.
23	Provision of à-la-carte channels or bouquet: (a) DRM (and SMS) shall be able to handle all the channels, made available on a platform, in à la carte mode.	Create number of channels on the platform, check if the same can be created on the DRM and SMS in à-la-carte.	Channel should be able to be created in à-la-carte in both SMS and DRM and a cross reference report can be generated from DRM and no exception found.
	(b) DRM (and SMS) shall have the capability to handle such number of broadcaster/DPO bouquets, as required by the DPO.	Create some broadcaster bouquets in the DRM and SMS. Also create some bouquets of the DPO in the DRM and SMS.	Both the DRM and SMS reflect the bouquets created.
24	DRM and SMS applications, along with their respective databases, shall be stored in such a way that they can be separately identified.	Check that DRM server does not have SMS and vice versa. Self-certification may be obtained. Note: This may be checked at actual deployed site or during regular audits.	

25	DRM shall have a provision to export the database/report for reconciliation with the SMS database. Further, there shall be a provision of reconciliation through secure APIs/secure scripts.	Export the database details/ report from DRM. Data from SMS may also be pulled and reconciled without manual intervention.	The DRM database is exported in entirety to the period and is in reconcilable format.
26	There shall be unique license key required for viewing, the encryption period for a specific key should be configurable to change at periodic interval in DRM deployed by DPO.	1. Review DRM system settings for license key management. 2. Verify that a unique license key is issued per device/user. 3. Check configuration options for setting and adjusting encryption period. 4. Review logs or perform a test to confirm periodic license key changes based on configuration.	1. DRM issues a unique license key per device/user. 2. Encryption period for keys is configurable. 3. Key change is performed automatically at the configured interval. 4. System logs confirm license key issuance and periodic updates.
27	For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB/unique consumer subscription from any other source other than the one specified by the IPTV system.	1. Review DRM system process for handling channel change events. 2. Verify that fresh license keys are generated for every channel change. 3. Check encryption methods used for license keys. 4. Perform a test to ensure license keys are delivered only through the authorized IPTV path and not from any unauthorized source. 5. Review security audit reports if available.	1. Fresh license keys are issued by DRM on each channel change. 2. License keys are securely encrypted. 3. License keys are received only from authorized IPTV system sources. 4. No license key leakage or unauthorized distribution detected.
28	DRM servers should comply with extant Rules and Regulations including relevant clause under extant provisions (if any) relating to data localisation, data security and privacy. It should not be allowed to connect main DRM server to some other location (India or other country) with some proxy or another server to	1. Review DRM system deployment architecture and network topology. 2. Verify that all DRM servers are physically located in India as per data localisation norms. 3. Check firewall and routing configurations to ensure no unauthorized proxy or remote server connection exists. 4. Review compliance certificates or audit	1. DRM servers are deployed within India and comply with data localisation laws. 2. No unauthorized proxy or remote server connections are present. 3. System design and network checks confirm compliance with data security and privacy norms. 4. Compliance

	integrate with SMS and DPO system.	reports for data localisation, security, and privacy requirements.	certificates/audit reports validate adherence to regulations.
29	IPTV service delivery may conform to multicast and/or unicast mode. The system configuration should ensure that every television channel is available to every customer on selection to view, irrespective of the mode of delivery or the number of viewers seeking such channel at any point of time. STBs/unique consumer subscription with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device or delivered to any other network in any manner whatsoever.	1. Verify IPTV system supports both multicast and unicast delivery modes. 2. Test channel availability on user selection under both modes, with multiple concurrent viewers. 3. Review STB/consumer device specifications for copy protection mechanisms. 4. Attempt to transfer recorded content to another device/network and observe the behavior. 5. Check DRM enforcement of copy protection policies on recorded content.	1. Every channel is available to all customers on-demand in multicast/unicast modes. 2. No service disruption regardless of viewer load. 3. STBs/consumer devices have active copy protection systems. 4. Recorded content cannot be transferred or shared externally. 5. DRM enforces copy protection on recorded programs.
30	IPTV system should not be allowed to deliver linear content to any other device except STB/unique consumer subscription which has been whitelisted in DRM.	1. Review DRM whitelist configuration for authorized STBs/unique consumer subscriptions. 2. Attempt to access linear content using a non-whitelisted or unauthorized device. 3. Observe content access behavior and check system logs for unauthorized access attempts. 4. Verify DRM enforcement on access restrictions to non-whitelisted devices.	1. Only whitelisted STBs/unique consumer subscriptions can access linear content. 2. Unauthorized devices are denied access. 3. DRM logs unauthorized access attempts, if any. 4. Content delivery strictly restricted as per whitelist.

31	The DRM should have following features: (a) It should restrict user to editing. (b) It should restrict user from sharing or forwarding or mirroring the content from the STB/unique consumer subscription. (c) It should disallow user to take screen shots or screen grabs or screen-recording, if technically feasible. (d) It should lock access to authorized STBs/unique consumer subscriptions only. (e) It should have Geo blocking feature. (f) It should be able to set expiry date to recorded content at STB/unique consumer subscription end based on various policies.	1. Review DRM technical documentation for feature support. 2. Test editing, sharing, forwarding, and mirroring protections on STB/device. 3. Attempt to take screenshots or screen recordings and observe system behavior. 4. Verify that only whitelisted STBs/consumer subscriptions can access content. 5. Check DRM system for Geo-blocking settings and perform geo-location testing. 6. Verify policy configuration for expiry dates on recorded content and test expiry behavior.	1. DRM restricts editing, sharing, forwarding, and mirroring effectively. 2. Screenshots/screen recording are blocked (if technically feasible). 3. Only authorized STBs/devices can access content. 4. Geo-blocking is active and functional. 5. Expiry dates on recorded content work according to policies set.
32	The DRM should have the capability of being upgraded over-the-air (OTA) so that the connected STBs/unique consumer subscription always have the most upgraded version of the DRM.	1. Review DRM system architecture for OTA upgrade capability. 2. Check documentation/process for DRM version management and OTA upgrade deployment. 3. Perform or observe a test OTA upgrade process on a sample STB/consumer device. 4. Verify that devices receive and apply updates without user intervention and without service disruption. 5. Review logs confirming successful upgrade deployment across devices.	1. DRM supports OTA upgrades. 2. OTA upgrade is smooth, automatic, and does not require manual intervention. 3. Devices are updated to the latest DRM version. 4. No service disruption occurs during or after the upgrade. 5. System logs record successful OTA updates.
33	The DPO shall ensure that the DRM is up to date by installing necessary patches, error corrections, additions, version releases, etc. so as to ensure protection of	1. Review system update logs and patch management process. 2. Verify records of applied updates and their timelines. 3. Check current DRM	1. DRM is up-to-date with latest patches and releases. 2. Updates applied regularly to maintain security and functionality.

	channels and content at all times	version against the latest available version.	
34	No such functionality should be added to or removed from the DRM which compromises security of channels. DPO shall be responsible for encryption of channels' signals before their delivery through its IPTV platform using DRM hybrid STBs/unique consumer subscription. All costs / expenses (by whatever name called) that are required to be incurred or become payable for such upgradation and for delivery/distribution of multi channel television programmes to subscribers shall be borne solely by such DPO. The DPO shall employ all reasonable security systems and procedures to prevent any loss, theft, piracy, un-authorized use, reception or copying of channels or any part thereof and shall notify broadcasters as soon as practicable after it becomes aware that such an event has occurred	1. Review change management process documentation. 2. Inspect recent changes to DRM settings for compliance. 3. Verify encryption processes on channel signals.	1. No unauthorized functionality changes found. 2. Encryption of channels is enforced properly. 3. Prompt reporting system to broadcasters exists.
35	The DRM should not in any way interfere with / invalidate fingerprinting.	1. Perform tests by triggering fingerprinting on content. 2. Observe if DRM affects visibility or functionality of fingerprinting.	1. Fingerprinting remains intact and functional. 2. No interference by DRM.
36	DPO shall promptly, and at it sole cost and expense, correct any issues with the DRM (such as bugs, defects, omissions or the like) that prevents subscribers from accessing the DRM hybrid STBs/unique consumer subscription or channels through the	1. Review ticketing/incident management system for DRM issues. 2. Confirm resolution timelines and closure reports.	1. Bugs/defects fixed promptly. 2. No cost implications for broadcasters.

	DRM hybrid STBs/unique consumer subscription.		
37	DPO shall provide broadcasters with video and audio codecs supported by the DRM hybrid STBs/unique consumer subscription. The DPO shall ensure that no such changes/modifications are made to such codecs parameters that will require broadcasters to incur any expense for delivery of channels / content that are free from viewer discernible problems (including, without limitation, video with no audio, audio with no video or significant signal distortion	1. Request list of supported codecs. 2. Review any changes to codec parameters. 3. Validate broadcaster's content delivery compatibility.	1. Supported codecs list shared. 2. No changes causing additional broadcaster cost. 3. No viewer-discernible quality issues.
38	DRM should ensure that the hybrid STBs/unique consumer subscription are verifiably located within India by reference to internet protocol address and service address. DRM must ensure and lock the viewership to single device by single STB/unique consumer subscription or any device by ensuring MAC ID based authentication. The DRM must use industry-standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.	1. Review DRM's IP tracking and MAC ID authentication setup. 2. Perform geo-location and proxy-bypass tests.	1. Devices locked to Indian IPs and MAC IDs. 2. Proxies blocked. 3. No unauthorized access from outside India.
39	DRM should ensure that television channels are accessible on STBs/unique consumer subscription of only such subscribers who are then-current,	1. Test subscription status validation process. 2. Attempt access from expired or invalid accounts.	1. Channels delivered only to active subscribers. 2. Access denied for inactive/invalid accounts.

	valid subscribers of the DPO, and such confirmation must take place prior to the DRM delivering (or authorizing the delivery of) television channel to the STBs/unique consumer subscription of such subscribers.		
40	Upon deactivation of any subscriber from the SMS, the DRM shall restrict delivery of all programme/services to that subscriber.	1. Deactivate a test subscriber in SMS. 2. Verify content access is immediately blocked.	1. DRM stops service immediately upon SMS deactivation.
41	The DRM should not have any feature to insert any content (including advertisement, banner on portion of screen, etc) by itself. However, ticker messages for consumer information as regards their services from DPO shall be permitted.	1. Review DRM system behavior during content playback. 2. Check for unauthorized insertions.	1. No ad/banner insertion by DRM. 2. Only authorized ticker messages appear.
42	The DRM should not mask/remove any copyright, trademark or any other proprietary information on the channels at the time of their delivery.	1. Test content flow and verify visible proprietary marks during playback. 2. Inspect watermarking/copyright info preservation.	1. All copyright/trademark marks preserved. 2. No masking or removal observed.

C. DRM Requirements in so far as they relate to fingerprinting for IPTV services (as per Schedule-X notified by TRAI on 14-09-2023)

Clause No	Requirement	Test Procedure	Test Results Expected
1	The DPO shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals	1. Review the DPO's documented fingerprinting policy and procedures. 2. Check fingerprinting system setup and scheduling configurations. 3. Observe or simulate fingerprinting execution at scheduled intervals. 4. Review logs and reports of past fingerprinting activities.	1. Fingerprinting is configured to run at regular, predefined intervals. 2. Logs and reports show consistent execution without manual intervention. 3. System, processes, and controls are in place to ensure continuity.
2	The STB/unique consumer subscription should support both visible and covert types of finger printing.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5 repetition and random position.	FP should appear on all the targeted STBs each time.
3	The fingerprinting should not get invalidated by use of any device or software.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5	FP should appear each time on all screens and should not be deactivated even if any key on remote or STB is pressed.

		repetition and random position.	
4	The fingerprinting should not be removable by pressing any key on the remote of STB/unique consumer subscription.	Enable fingerprinting on the STB/unique consumer subscription using SMS/DRM control or configuration settings. Once the fingerprint appears on the screen during content playback, press each of the keys on the remote control (including volume, menu, back, info, mute, etc.) one at a time, observing the screen each time. Repeat the above test across multiple STB models (if available) to ensure consistent behavior. Log the commands sent and observe system behavior in terms of: Fingerprinting visibility Any interruption or disappearance of fingerprint	The fingerprint remains visible on the screen regardless of any key press on the remote control. No combination or sequence of remote key presses should result in: Hiding Removing Shifting off-screen Temporarily disabling the fingerprint The position, size, and visibility of the fingerprint must remain unaffected and persistent throughout playback.

5	The finger printing should be on the topmost layer of the video.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5 repetition and random position.	FP should appear on the video and be visible.
6	The finger printing should be such that it can identify the unique STB/unique consumer subscription number or the unique VC number or the MAC ID.	1. Trigger fingerprinting on sample content across different STBs/unique consumer devices. 2. Verify that the fingerprint displayed includes the correct STB number, VC number, or MAC ID. 3. Cross-check displayed IDs against subscriber management records.	1. Fingerprinting correctly displays the unique STB/VC/MAC ID. 2. IDs are accurate and match SMS records. 3. No mismatch or missing identification information.
7	The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen, and games etc.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5 repetition and random position.	FP should appear each time on all screens of STB in all scenarios mentioned in the clause.

8	The location, font color and background color of fingerprint should be changeable from head end and should be random on the viewing device.	1. Review headend configuration options for fingerprint settings. 2. Change location, font color, and background color settings. 3. Observe fingerprint behavior on multiple STBs/unique consumer devices. 4. Verify randomness of fingerprint placement during viewing.	1. Location, font color, and background color are configurable from headend. 2. Fingerprint appears at random locations on viewing devices. 3. Changes are reflected in real-time or as per set schedule.
9	The finger printing should be able to give the numbers of characters as to identify the unique STB/unique consumer subscription and/or the MAC ID.	1. Observe fingerprint display during content playback. 2. Check that sufficient characters are shown to uniquely identify the device/user. 3. Match fingerprint information against SMS/DRM records.	1. Fingerprint displays enough characters to uniquely identify each subscriber/device. 2. No duplication or confusion between different subscribers.
10	The finger printing should be possible on global as well as on the individual STB/unique consumer subscription basis.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5 repetition and random position.	FP should appear each time as per schedule on specific STBs and all STBs.

11	The overt fingerprinting/watermarking should be displayed by the DPO without any alteration with regard to the time, location, duration and frequency.	1. Schedule and trigger fingerprinting as per standard parameters. 2. Monitor fingerprint display across multiple devices. 3. Verify that time, location, duration, and frequency match predefined settings without alteration.	1. Fingerprinting/watermarking appears exactly as configured. 2. No deviations in time, location, duration, or frequency.
12	The DRM deployed should be able to generate fingerprinting/watermarking both global fingerprinting as well as targeted channel fingerprinting/watermarking.	1. Initiate global fingerprinting across all channels. 2. Initiate targeted fingerprinting on selected channels. 3. Verify correct application of fingerprinting in both scenarios.	1. Global fingerprinting is applied across all channels. 2. Targeted fingerprinting is successfully limited to specific channels.
13	The DRM shall support and enable forensic watermarking at STB/unique consumer subscription level.	1. Check DRM system configuration for forensic watermarking capability. 2. Trigger forensic watermarking for a specific STB/unique consumer device. 3. Validate insertion of unique forensic watermark in content stream.	1. Forensic watermarking is active at individual STB/unique consumer subscription level. 2. Watermarks are unique per subscriber/device.

14	The DRM shall have the capability to run fingerprinting with at least one fingerprinting every ten (10) minutes on a 24x7x365 basis. DRM should have a feature to publish report of fingerprinting schedule for defined interval. The DPO shall make such report available to broadcaster on request.	1. Send Global Fingerprinting command from SMS with 5 repetition and random position. 2. Send unique/ individual Fingerprinting command from SMS with 5 repetition and random position.	FP should appear as scheduled each time on the boxes and it should change its location on all schedules.

D. DRM Requirements in so far as they relate to STBs/unique consumer subscription (as per Schedule-X notified by TRAI on 14-09-2023)

Clause No	Requirement	Test Procedure	Test Results Expected
1	All STBs/unique consumer subscription should have a DRM content protection.	1. Verify DRM client integration in STBs/unique consumer subscriptions. 2. Test playback of encrypted content. 3. Check for successful DRM license acquisition and enforcement.	1. DRM content protection is active on all STBs/unique consumer subscriptions. 2. Unauthorized content playback is not possible.
2	The STB/unique consumer subscription deployed should be capable to support content decryption, decoding and DRM license evaluation.	1. Deliver encrypted content to the STB/unique consumer subscription. 2. Monitor decryption, decoding, and license validation process. 3. Validate playback after successful license evaluation.	1. STB/unique consumer subscription decrypts, decodes, and evaluates DRM licenses correctly. 2. Content plays only after proper license validation.
3	The STB/unique consumer subscription should be capable of displaying fingerprinting inserted from Headend through DRM/SMS. The STB/unique consumer subscription should support both targeted channel fingerprinting as well as all global fingerprinting.	1. Trigger global and targeted fingerprinting from the Headend. 2. Observe fingerprint display on STBs/unique consumer subscriptions. 3. Verify fingerprint visibility across content.	1. STBs/unique consumer subscriptions correctly display both global and targeted fingerprints. 2. Fingerprints are visible, accurate, and tamper-proof.
4	The STB/unique consumer subscription should be individually addressable from the Head-end.	1. Send individual commands (e.g., activation, deactivation, entitlement updates) from Headend to specific STBs/unique consumer subscriptions. 2. Monitor response and execution on target devices.	1. Each STB/unique consumer subscription responds individually to Headend commands. 2. No impact on non-targeted devices.

5	The STB/unique consumer subscription should be able to receive messages from the Head-end.	1.From the SMS/DRM Head-end system, compose and send a test message (e.g., "Test Broadcast Message") to: -A specific STB/unique consumer subscription -A group of STBs -All STBs (broadcast message) 2.Ensure the STB/unique consumer subscription is powered on and tuned to a channel. 3.Monitor the STB screen for the delivery of the message. 4.Verify that: -The message appears clearly on the screen. -It is readable and properly formatted. -It is received within an acceptable time frame (e.g., within a few seconds).	The STB/unique consumer subscription successfully receives the message sent from the Head-end. The message is displayed correctly on the screen with no distortion or truncation. No loss or delay in delivery beyond expected limits. Message content remains unaltered and visible for the configured duration.
6	The messaging character length should be minimal of upto120 characters.	Send a message from the Headend with 120 characters to STB/unique consumer subscription.	Message of 120 characters displays correctly without truncation or error.
7	There should be provision for global messaging, group messaging and the individual STB/unique consumer subscription messaging.	Send global, group, and individual messages from the Headend; verify reception.	Messages are received correctly for each type without error.
8	The STB/unique consumer subscription must be compliant to the applicable Bureau of Indian Standards	Review STB/unique consumer subscription BIS certification.	BIS compliance certificates are available and valid.
9	The STBs/unique consumer subscription should be addressable over the air to facilitate OTA software upgrade.	Push OTA update to the STB/unique consumer subscription; monitor update process.	OTA software upgrade completes successfully without manual intervention.
10	The STBs/unique consumer subscription with facilities for recording the programs shall have international standard copy protection system	Attempt to record and export content from STB/unique consumer subscription; verify protection mechanisms.	Recorded content cannot be exported or misused; copy protection is active.

11	The STB/unique consumer subscription should have a provision that fingerprinting is never disabled.	Try to disable fingerprinting at STB/unique consumer subscription settings.	Fingerprinting feature remains enabled and active at all times.
12	The watermarking network logo for all pay channels shall be inserted at encoder end only.	Verify source of watermark on pay channels through content stream analysis.	Watermarking is verified to originate at encoder end only.
13	DRM/SMS deployed should be able to send scroll messaging which should be only available in the lower part of the screen.	Send scroll message and observe screen location.	Scroll messaging appears only at the lower part of the screen.
14	DRM deployed should be able to geo tag STB/unique consumer subscription deployed in the network for security.	Check DRM logs and device information for geotagging details.	STBs/unique consumer subscriptions are geo-tagged and location information is recorded.
15	STB/unique consumer subscription should take all commands directly from DRM not from any intermediate servers.	Trace command routing from DRM to STB/unique consumer subscription.	Commands are received directly from DRM without intermediaries.
16	STB/unique consumer subscription while using IPTV infrastructure should not have feature to download (direct or side download) any 3rd party App/APK and should not have access to any browser.	Attempt side-loading APKs or accessing browser.	All such unauthorized downloads and browser access are blocked.
17	STB/unique consumer subscription should not be able to access the authorization keys from any other source except from the IPTV system through the IPTV closed network. DRM must ensure that the authorization keys are not received by the STB/unique consumer subscription from any other source other than the one specified by the IPTV system	Attempt to receive keys from external sources.	STB/unique consumer subscription receives keys only via IPTV closed network.
18	No play store should be accessible for enabling download, etc. when STB/unique consumer subscription, is	Try accessing Play Store from STB/unique consumer subscription.	Play Store and similar download portals are blocked.

	functioning in the IPTV network.		
19	STB/unique consumer subscription should have copy protection.	Attempt to copy/export content from STB/unique consumer subscription.	Copy protection prevents unauthorized copying.
20	DPO system should have capability to maintain un-editable logs of all activity and configurations including download or upgrade of IPTV services App (if any) at STB/unique consumer subscription end	Review activity logs for completeness and edit history.	Logs are complete, detailed, and tamper-proof.
21	The DRM should not allow delivering linear TV channels on Internet. The delivery of multi channel television programmes should remain in a closed network within the device.	Monitor content stream paths and access points.	No Internet-based delivery; content restricted to closed IPTV network.
22	The STB/unique consumer subscription should have forced messaging capability including forced finger printing display.	Trigger forced message and fingerprint from Headend.	Forced message and fingerprint appear on STB/unique consumer subscription without user control.
23	The DRM hybrid STBs/unique consumer subscription should be tested for the following prior to their seeding in the subscribers' premises: (a) System down testing (b) Error messaging (c) Negative user journey testing (d) Device variance testing (e) Destructive testing (f) Application monitoring testing (g) In-app monitoring testing	Conduct each type of testing and document outcomes.	All test scenarios pass with system handling failures gracefully and maintaining security and functionality.

J. Summary of Test Results: (to be filled by testing team)

GR/ IR No.: *Schedule-X of TRAI Notification dated 14-09-2023*

Test Guide No.: *TEC XXXXX:2025*

Equipment name & Model No._____

Clause No.	***Compliance*** *(Complied/Not Complied/ Submitted/Not Submitted/Not Applicable)*	***Remarks / Test Report Annexure No.***

Date:

Place:

Signature & Name of TEC testing Officer /

*** Signature of Applicant / Authorized Signatory**

***** ***Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results alongwith Form-A. The Authorised signatory shall be the same as the one for Form 'A'.***

K. Annexure (to be filled by testing team)

(Please provide the clause wise test procedure for specific Lab tests)

L. List of Abbreviations

Abbreviation	Expanded Form
API	Application Programming Interface
CAS	Conditional Access System
DB	Database
DPO	Distribution Platform Operator
EPG	Electronic Programme Guide
FP	Finger Printing
FTA	Free-To-Air
GUI	Graphical User Interface
LCN	Logical Channel Number
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over-The-Air
OTT	Over-The-Top
PIN	Postal Index Number
PSI/ SI	Program Specification Information / System Information
SLA	Service-Level Arrangement
SMS	Subscriber Management System
STB	Set Top Box
TEC	Telecommunication Engineering Centre
TRAI	Telecom Regulatory Authority of India
UA	Unique Access
UI	User Interface

Annexure

Template for submitting Comments or Feedback

[Comments on each section/sub section/table/figure etc be stated in a fresh row. Information/comments should include reasons for comments and suggestions for modified wordings of the clause]

Name of Commentator/Organization ……..

S. No.	Section of the Draft test Guide	Clause/Para/Table/ Figure No. of draft Test Guide	Comments/ Suggested modified Wordings	Justification for proposed Change
1.				
2.				
3.				
4.				
5.				
6				
7.				
8.				
9.				
10.				

Note- a) Kindly insert more rows as necessary for each clause/table, etc.

b) Comments may be sent in electronic form to jto-cb@gov.in, with a copy to dircb2.tec-dot@gov.in**.** & ddgcb.tec@gov.in , by 23-07-2025**.**

Name:
Email:
Mobile: