DAS Audit and Report Generation as per extant TRAI Regulations

Date: 6th August 2025
Venue: TRAI HQ

Prateek Katoch
(Sr, Manager- BECIL)

THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (No. 1 of 2017) and amendments thereafter

Introduction

- Broadcast Engineering Consultants India Limited (BECIL) an ISO 9001:2015, ISO 27001:2013, ISO/IEC 20000-1:2018 and CMMIL3 certified, a Mini Ratna Central Public Sector Enterprise (CPSE) under Ministry of Information & Broadcasting.

- BECIL has been conducting the audit of Digital Addressable System (DAS) of DPOs (CATV/DTH/HITS/IPTV) for conformity to TRAI Interconnection Regulations since 2010.

- These DAS audits conducted to check conformity of the components of DAS (CAS, SMS, STB etc) to the parameters specified in the TRAI Regulations.

- As per extant Regulations of 2017 (applicable since 2019) all DPOs are required to get their DAS audited once in a calendar year by BECIL or TRAI empaneled agencies.

- The detailed audit is carried out as per procedures specified in the Audit Manual issued by TRAI.

Key Discussion Points

1. **Audit under section 10 Of TRAI Regulations**

2. **Audit Methodology and Scope of work**

3. **Documents Requirement**

4. **Schedule III Compliance Checks**

5. **Audit under section 15 of TRAI Interconnection Regulations**
   1. **Documents Requirement**
   2. **Data extraction Procedure**
   3. **Analysis of Data**

6. **TS Recording and Field Inspection During Audit**

7. **Key points to be checked while conducting audit**

8. **Audit Report Generation as per audit manual.**

Audit Under section 10

- Schedule III compliance of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (No. 1 of 2017).

- Two instances under which these audits can be conducted. (DPO Caused)
  - Case 1: When DPO wants to seek pay channels from broadcasters.

  - Case 2: When the DPO already have pay channel content and wants to ensure its DAS system compliance.

- Audit under section 10 can also be caused by broadcasters if he is of the opinion that the DPO system does not meet the regulatory requirements.

Audit Methodology and scope of work

- Perform walk-through of the main head-end/s where CAS and SMS servers are deployed.

- Obtain Headend diagram and validate with the equipment installed in the head-end/s.

- Use FTA cable box/ TS analyzer to confirm whether all channels are encrypted

- Walkthrough and understanding the customer acquisition Process and verification of sample CAF and PAF Forms available with DPO.

- Verification of TRAI interconnection Schedule III Compliance of the DPO DAS System (CAS, SMS Fingerprinting and STB) as per procedure mentioned in Section 7 of the Audit Manual.

Documents Requirement

- Valid DAS license/ permission issued by Ministry of Information and Broadcasting (MIB)

- BIS certificates for all makes & models of STB deployed by DPO after DAS implementation.

- Certificate from all the CAS vendors .

- Certificate from SMS vendors .

- Block Schematic diagram of Head-end including CAS and SMS.

- Signed and stamped copy of compliance audit form.

- Certificate from STB vendor

- Sample Copies CAF and PAF forms filled by customers

- List of all the decoder along with VC serial numbers issued by broadcasters to DPO.

Schedule III Compliance Checks

Three types of compliance checks are required as per TRAI Regulations:

1. CAS and SMS Requirements
2. Fingerprinting Requirements
3. STB Requirements

CAS and SMS Requirements

Regulatory Provisions	Audit Procedure
Schedule III – C1 The distributor of television channels shall ensure that the current version of the CAS, in use, do not have any history of hacking.	• DPO to provide certificate from each CAS vendor
Schedule III – C2 The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.	• DPO to provide certificate from each SMS vendor • Auditor to check, verify and document whether all the actions, including but not limited to activation, de-activation, package creation, package change/modification, FP insertion, and scroll insertion are being recorded in SMS.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C3 It shall not be possible to alter the data and logs recorded in the CAS and the SMS.	• Simulation test should be carried on one model of every STB available in the inventory of DPOs. • The logs of these activities then are required to be cross checked both in CAS and SMS. • Once extracted or downloaded to any format these logs can be editable.
Schedule III – C4 The distributor of television channels shall validate that the CAS, in use, do not have facility to activate and deactivate a Set Top Box (STB) directly from the CAS terminal. All activation and deactivation of STBs shall be done with the commands of the SMS.	• DPO/ CAS vendor to provide declaration and demonstrate the activation procedure. • The DPO can only active/de-activate directly from CAS only for testing purpose.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C5 The SMS and the CAS should be integrated in such a manner that activation and deactivation of STB happen simultaneously in both the systems.	• Simulation test should be carried on one model of every STB available in the inventory of DPOs.
Schedule III – C6 The distributor of television channels shall validate that the CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded.	• Required declaration certificate from CAS Vendor
Schedule III – C7 The fingerprinting should not get invalidated by use of any device or software.	• Auditor should trigger a fingerprint (any one ECM/EMM) of minimum 180 seconds duration from SMS/CAS to the test STB. (minimum 180 seconds timeline is to ensure that fingerprinting command is still available on STB when it is rebooted as some of the STB takes at least 120 seconds to reboot).

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C8 The CAS and the SMS should be able to activate or deactivate services or STBs of at least 10% of the subscriber base of the distributor within 24 hours.	• Declaration Certificate required from CAS and SMS Vendors
Schedule III – C9 The STB and Viewing Card (VC) shall be paired from the SMS to ensure security of the channel.	• Auditor should verify that paired VC of one STB should not work with another STB • Auditor to interchange VC between two STBs of the DPO and confirm that both STBs give error message on-screen. • Only applicable in case of carded STBs.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C10 The CAS and SMS should be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB by STB basis.	• Simulation test should be carried on one model of every STB available in the inventory of DPOs.
Schedule III – C11 The SMS should be computerized and capable of recording the vital 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 k. Unique VC number	• Create one test customers in SMS with dummy names . • Allocate fresh hardware and map the test customer to an LCO • Check whether item "a to k" specified in Sch-III A(11) are getting captured.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C12 The SMS should be capable of: a. Viewing and printing of historical data in terms of the activations and the deactivations of STBs. b. Locating each and every STB and VC installed. c. Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.	• The Auditor will check the SMS capability of capturing this information in SMS at any desired time from the front end (SMS application) of the SMS. • The auditor on sample basis will also generate one report from the SMS database (back end) also and verify the information captured through the front end of SMS application.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C13 The SMS should be capable of generating reports, at any desired time about: i. The total number of registered subscribers. ii. The total number of active subscribers. iii. The total number of temporary suspended subscribers. iv. The total number of deactivated subscribers. v. List of blacklisted STBs in the system. vi. Channel and bouquet wise monthly subscription report in the prescribed format. vii. The names of the channels forming part of each bouquet. viii. The total number of active subscribers subscribing to a particular channel or bouquet at a given time. ix. The name of a-la carte channel and bouquet subscribed by a subscriber. x. The ageing report for subscription of a particular channel or bouquet.	• The Auditor will check the generation capability of these reports in SMS at any desired time from the front end (SMS application) of the SMS. • The auditor on sample basis will also generate two report from the SMS database (back end) also and verify these reports with the reports generated from SMS application. • Date & time stamp is mandatory in report generation.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C14 The CAS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the CAS including but not limited to activation and deactivation commands issued by the SMS.	• Check and generate the transaction logs of last two years to verify the CAS capability.
Schedule III – C15 The CAS shall be able to tag and blacklist VC numbers and STB numbers that have been involved in piracy in the past to ensure that such VC or the STB cannot be re-deployed.	• Auditor to blacklist one STB & VC of each CAS, and check the status of the STB+VC in CAS

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C16 It shall be possible to generate the following reports from the logs of the CAS: STB-VC Pairing / De-Pairing STB Activation / De-activation Channels Assignment to STB Report of the activations or the deactivations of a particular channel for a given period.	• Auditor will generate these reports from the CAS. • STB VC pairing de-pairing report is applicable only for carded CAS. • All reports to be extracted in such a manner that no STB/VC is left out from the database
Schedule III – C17 The SMS shall be capable of generating bills for each subscriber with itemized details such as the number of channels subscribed, the network capacity fee for the channels subscribed, the rental amount for the customer premises equipment, charges for pay channel and bouquet of pay channels along	• On sample basis, Auditor to verify the Itemized bill generated from the SMS to ensure that it captures all the mentioned details in this clause & record a copy of the bill format & any discrepancy noticed, if any, in the audit report.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C 18 The distributor shall ensure that the CAS and SMS vendors have the technical capability in India to maintain the systems on 24x7 basis throughout the year.	a) Auditor to check that the CAS declaration from each CAS vendor **(Annexure 1)** mentions the availability of this facility. b) Auditor to check that the SMS declaration **(Annexure 2)** from each SMS vendor mentions the availability of this facility.
Schedule III – C 19 The distributor of television channels shall declare the details of the CAS and the SMS deployed for	a) DPO to declare on its letterhead the no. of CAS systems and SMS deployed in each of its distribution networks. It should mention the no. of "Headends" connected with the said CAS and SMS. This declaration is to be signed by authorized signatory/compliance officer. (Annexure 3) a) Any changes in CAS and SMS and STB should be reported by DPO and can be verified by auditor.

CAS and SMS Requirements contd.

Regulatory Provisions	Audit Procedure
Schedule III – C 20 Upon deactivation of any subscriber from the SMS, all program/ services shall be denied to that subscriber.	• Auditor to deactivate the "test subscribers" from the SMS and confirm the corresponding STB is deactivated for all channels / services including DD channels.
Schedule III – C 21 The distributor of television channels shall preserve unedited data of the CAS and the SMS for at least two years.	In case of distribution platforms operational for less than 2 years, the Auditor to check that the CAS declaration from each CAS vendor **(Annexure 1)** mentions the CAS is compliant with this requirement. b) In case of distribution platforms operational for less than 2 years, the Auditor to check that the SMS declaration **(Annexure 2)** from each SMS vendor mentions the SMS is compliant with this requirement. c) Auditor to take declaration from DPO that it has preserved unedited data of the CAS and the SMS for at least two years if the CAS and SMS system are

Fingerprinting Requirements (Schedule III)

Regulatory Provisions	Audit Procedure
Schedule III – D1 The distributor of television channels shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals	Auditor to trigger fingerprinting from SMS by inputting start / end time, duration of display, frequency of display and confirming that the fingerprint is seen on the test STB output. Auditor to take a screenshot of the fingerprint.
Schedule III – D2 The STB should support both visible and covert types of finger printing. The fingerprinting should not get invalidated by use of any device or software. Provided that only the STB deployed after coming into effect of the Amendment Regulations shall support the covert finger printing.	For visible type of finger printing: same as 1 above b) For covert type: Auditor should ensure this capability is mentioned in STB certificate **(Annexure 4)** and as well test the same feature during audit. c) Auditor should accept any type of covert fingerprinting.

Fingerprinting Requirements (Schedule III)............Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 3 The fingerprinting should not get invalidated by use of any device or software.	Auditor should trigger a fingerprint (any one ECM/EMM) of minimum 180 seconds duration from SMS/CAS to the test STB (minimum 180 seconds timeline is to ensure that fingerprinting command is still available on STB when it is rebooted as some of the STB takes at least 120 seconds to reboot). b) In case the CAS does not have provisions to send minimum 120 seconds FP then multiple commands of FP of short duration may be sent to verify the same. d) The STB should be rebooted, and fingerprint should reappear again automatically. If fingerprint disappears, auditor should take appropriate note.

Fingerprinting Requirements (Schedule III)...........Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 4 The fingerprinting should not be removable by pressing any key on the remote of STB.	Auditor should trigger a fingerprint of at least 120 seconds or above duration from SMS/ CAS to the test STB.
Schedule III – D 5 The finger printing should be on the top most layer of the video.	b) While fingerprint is displayed on STB output connected to TV screen, auditor should press every key on the STB remote control and STB front panel. c) Auditor should confirm that no action while pressing buttons on remote or on STB box (soft boot or hard boot) makes the displayed fingerprint disappear even momentarily for the whole duration of FP. d) If fingerprint disappears with any key action, this requirement is not complied with. e) If may be noted that in case if FP more than 60

Fingerprinting Requirements (Schedule III)............Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 6 The finger printing should be such that it can identify the unique STB number or the unique VC number.	Auditor should trigger fingerprint on two test STBs and confirm the fingerprint displayed are unique to the VCs in the STBs (UA no. in card-less STBs).
Schedule III – D 7 The fingerprinting should appear on the screens in all scenarios, such as menu, Electronic Program Guide (EPG), Settings, blank screen, and games etc,	a) Auditor should trigger 120 seconds or more duration fingerprint on test STB and use remote control of STB to navigate to Menu page, EPG page, Settings page, Blank screen and Games page. b) Fingerprint should be displayed on all the above-mentioned pages.

Fingerprinting Requirements (Schedule III)…………Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 8 The location, font color and background color of fingerprint should be changeable from head end and should be random on the viewing device.	Auditor should trigger fingerprint on test STB multiple times, each time with at least 3 different permutation/combinations of location, font color, and background box color. The locations of the fingerprint should be seen on random areas of the TV screen to make it unpredictable to viewer.
Schedule III – D 9 The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the VC.	• Auditor should trigger fingerprint on two test STBs and confirm the fingerprint displayed are corresponding uniquely to the actual VCs in the STBs (UA no. in cardless STBs).
Schedule III – D 10 The finger printing should be possible on global as well as on the individual STB basis.	Auditor should trigger fingerprint to all STBs and confirm fingerprints are displayed on all test STBs provided DPO has no objection while testing the feature of global FP on all its STBs. b) If DPO has objection then this feature can be

Fingerprinting Requirements (Schedule III)............Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 11 The overt fingerprinting should be displayed by the distributor of television channels without any alteration with regard to the time, location, duration and frequency.	Auditor should obtain fingerprint Schedules from some broadcaster channels distributed by the DPO. b) Auditor should monitor sample channels of those broadcaster on DPO's STB and take screenshot of broadcaster fingerprint seen on TV screen as proof of compliance
Schedule III – D 12 Scroll messaging should be only available in the lower part of the screen.	a) Auditor should trigger scroll message of 120 characters from the DPO's SMS or CAS targeted to all test STBs. b) The scroll should be displayed as a horizontally moving ticker on the lower part of the TV screen.

Fingerprinting Requirements (Schedule III)…………Contd.

Regulatory Provisions	Audit Procedure
Schedule III – D 13 The STB should have a provision that fingerprinting is never disabled.	a) Auditor should trigger a fingerprint of 120 seconds or more duration FP from SMS/ CAS to the test STB. b) The STB should be rebooted, and fingerprint should reappear again automatically. If fingerprint disappears, this requirement is not complied with. c) The STB declaration **(Annexure 4)** should also mention this capability.
Schedule III – D 14 The watermarking network logo for all pay channels shall be inserted at encoder end only. Provided that only the encoders deployed after coming into effect of the Amendment regulations shall support watermarking network logo for all pay channels at the	To confirm the network logo is inserted from the encoder end only for all channels: a) Auditor should disconnect all test STBs from RF signal and then observe the TV screen. b) If network logo is still visible on TV screen, then the requirement of insertion of network logo at the

STB Requirements (Schedule III)

Regulatory Provisions	Audit Procedure
Schedule III – E1 All STBs should have a Conditional Access System.	To inspect all models of STBs available in the inventory of MSOs or deployed (2 units of each make & model) under test and confirm the STB serial no./VC no./UA no. exists in the live CAS database.
Schedule III – E 2 The STB should be capable of decrypting the Conditional Access messages inserted by the Head-end.	• The auditor will check and verify whether the STB is able to execute all the commands initiated from the CAS whether activation/de-activation of particular channel or package or FP/messaging command without any major delay or issue.
Schedule III – E 3 The STB should be capable of doing fingerprinting. The STB should support both Entitlement Control Message (ECM) and Entitlement Management Message (EMM) based fingerprinting.	To trigger fingerprinting on a particular channel and confirm fingerprint is seen on all test STBs on that particular channel only at the same time. This is ECM based fingerprinting.

STB Requirements (Schedule III)............Contd.

Regulatory Provisions	Audit Procedure
Schedule III – E 4 The STB should be individually addressable from the Head-end.	The auditor will verify whether the STB are addressable by performing simulation tests on the STB for activation/de-activation.
Schedule III – E 5 The STB should be able to receive messages from the Head-end.	Auditor should trigger scroll message of 120 characters from the DPO's SMS targeted to all test STBs. b) The scroll should be displayed in its entirety as a horizontal moving ticker on the lower part of the TV screen.
Schedule III – E 6 The messaging character length should be minimal 120 characters.	Auditor should trigger scroll message of 120 characters from the DPO's SMS targeted to all test STBs. The scroll should be displayed in its entirety as a horizontal moving ticker on the lower part of the TV

STB Requirements (Schedule III)…………Contd.

Regulatory Provisions	Audit Procedure
Schedule III – E 7 There should be provision for global messaging, group messaging and the individual STB messaging	a) Auditor should trigger scroll to all STBs and confirm it is displayed on all test STBs. b) Auditor should trigger scroll to one test STB and confirm it is displayed on the particular STB only.
Schedule III – E 8 The STB should have forced messaging capability including forced finger printing display.	• Auditor should trigger scroll messaging from SMS or CAS to all STB in the network which should display the fingerprint as the message. Auditor should take screenshot of the display
Schedule III – E 9 The STB must be compliant to the applicable Bureau of Indian Standards	a) Auditor should take copies of BIS certificates from the DPO for each make & model of STB procured after 2012. b) The certificates should mention exact STB make & model nos.

STB Requirements (Schedule III)…………Contd.

Regulatory Provisions	Audit Procedure
Schedule III – E 10 The STBs should be addressable over the air to facilitate OTA software upgrade.	DPO shall give a declaration on its letterhead mentioning the availability of this facility.
Schedule III – E 11 The STBs with facilities for recording the programs shall have a copy protection system	Auditor to check and report: a) For STBs having recording facility to internal and/or external storage devices such as USB / Hard Disk drives, auditor should check recorded content plays only on the specific STB where content was recorded. b) Auditor to check that scheduled fingerprint and scroll messaging is displayed even when stored content is played on the STB. c) Auditor should confirm that recorded content cannot be played if STB is in de-active state

Audit Under section 15 of the TRAI Interconnection Regulations

- Minimum essential checks are required to verify the integration of CAS and SMS before conducting the MSR verification Process.

- Data extraction to be carried out after the ensuring the integration of the Systems

- 20% MSR dates of the audit period to be picked up randomly by the auditor for conducting the MSR verification w.r.t each broadcasters.

Documents Requirement under section 15 Audit

- Valid DAS license/ permission issued by Ministry of Information and Broadcasting.

- Block schematic diagram of Headend including CAS and SMS.

- Certificate from all the CAS vendors **(Format as in Annexure 1).**

- Certificate from SMS vendors **(Format as in Annexure 2).**

- Signed and stamped copy of subscription audit form as per **Annexure 5**.

- Monthly MSR reports of the audit period submitted to broadcasters.

- **Monthly SMS report regarding state wise active/de-active STB count for the audit period. This report is applicable for all DPOs.**

Data extraction Process under section 15

- *Extraction of as on date data dumps from the SMS and CAS server deployed by DPO.*

- *Analysis on the data dump to verify the 20% random sample weeks of the audit period in respect of monthly subscriber report submitted by DPO to every broadcaster. The auditor is required to verify the MSR data for every pay channel of broadcasters available on DPO's network for these 20% sample weeks selected on random basis by the auditor.*

- *Analysis on data dumps to verify the as on date active, de-active count of STBs available on the network of DPO.*

- *Analysis on data dump to report the active STB count on 5 random dates from the audit period other than 7th, 14th , 21st and 28th .*

Data extraction Process under section 15..........Contd.

- *As on date DPO package wise, a-la-carte and broadcaster bouquet wise STB/VC details (both from SMS & CAS system)*

- *Verification and reporting of Channel to package mapping along with service ID (with creation, modification and discontinue date) from SMS & CAS of the audit period.*

- *As on Date Reconciliation of VC and STB from complete CAS and SMS for the date of Audit. Any discrepancy of VC not active in SMS but found active in CAS, excluding test/monitoring VC/STB, or vice versa should be reported in Actual numbers as well as percentage of the total base.*

Analysis of Data
(VC To VC Reconciliation)

DATE	System Name	Active VC Count in CAS	Active VC Count in SMS	Active VC Count Matched CAS VS SMS	Active VC Count Matched SMS Vs CAS	CAS Vs SMS MISSING	SMS Vs CAS MISSING
17-Mar-19	Verimatrix	296158	296430	295483	295483	675	947
17-Mar-19	Cisco	1149338	1150641	1148223	1148223	1115	2418
		1445496	1447071	1443706	1443706	1790	3365
22-May-19	Verimatrix	292879	292352	290059	290059	2820	2293
22-May-19	Cisco	1082137	1086180	1080352	1080352	1785	5828
		1375016	1378532	1370411	1370411	4605	8121
1-Jul-19	Verimatrix	289994	276101	273167	273167	16827	2934
1-Jul-19	Cisco	990614	997514	975781	975781	14833	21733
		1280608	1273615	1248948	1248948	31660	24667
3-Oct-19	Verimatrix	302906	292802	288908	288908	13998	3894
3-Oct-19	Cisco	964936	965532	958738	958738	6198	6794
		1267842	1258334	1247646	1247646	20196	10688
11-Jan-20	Verimatrix	306123	301474	301115	301115	5008	359
11-Jan-20	Cisco	899530	899312	898231	898231	1299	1081
		1205653	1200786	1199346	1199346	6307	1440

(State wise Monthly active VC Count of Audit Period) from SMS

As on Date	STATE	ACTIVE VC COUNT	De-active VC Count (for last 90 days)
31-Mar-19	Andhra Pradesh	89909	75000
31-Mar-19	Karnataka	54689	50000
31-Mar-19	Telangana	57872	40000
31-Mar-19	Kerala	1244601	80000
30-Apr-19	Andhra Pradesh	82873	75000
30-Apr-19	Karnataka	52312	50000
30-Apr-19	Telangana	51198	40000
30-Apr-19	Kerala	1216377	80000

Data Analysis
(MSR Verification Table)

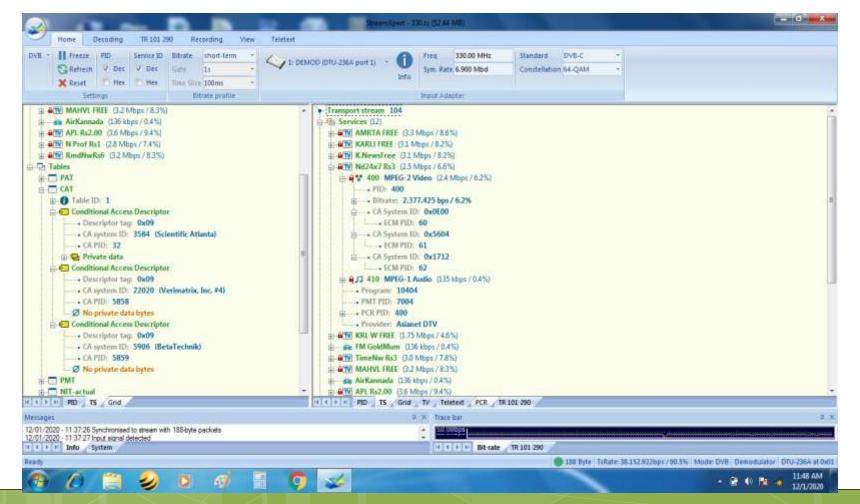| Name of Pack/Channel	Type	Broadcaster Name	Tag	Verified Count CAS (Verimatrix and CISCO)	Verified Count Zenith (SMS)	Reported MSR Count	Variation w.r.t Reported MSR Count
				A	B	C	D=Max (A,B)-C
Movies Now	Ala-carte	XYZ	MOVIES_NOW_NTO	13,997	13,742	13,993	4
Movies Now HD	Ala-carte	XYZ	HD_MOV_NOW_NTO	3,124	3,024	3,110	14
Romedy Now	Ala-carte	XYZ	ROMEDY_NOW_NTO	6,149	6,056	6,134	15
MNX	Ala-carte	XYZ	MNX_NTO	6,013	5,902	6,003	10
Times Now	Ala-carte	XYZ	TIMES_NOW_NTO	10,845	9,950	10,834	11
BOUQUET-1	Bouquet	XYZ	TIMES_BOQ1_NTO	67	843	67	776
BOUQUET-2	Bouquet	XYZ	TIMES_SD02_KER_NTO	722,470	691,387	707,954	14,516
BOUQUET-3	Bouquet	XYZ	TIMES_HD_BOQ3_NTO	22,743	19,481	22,742	1

TS Recording and Field Inspection

- For carrying out the TS recording , a good quality TS recorder device is required for analysis of TS streams configured in the network.

- TS recording should be carried out in the Headend as well as at random two locations in the field.

- If broadcaster has provided recorded TS streams and ground VC samples than the same needs to be verified during the conduct of audit.

- Random Sample TS screenshots of TS configured should be enclosed with the audit report to substantiate the findings.
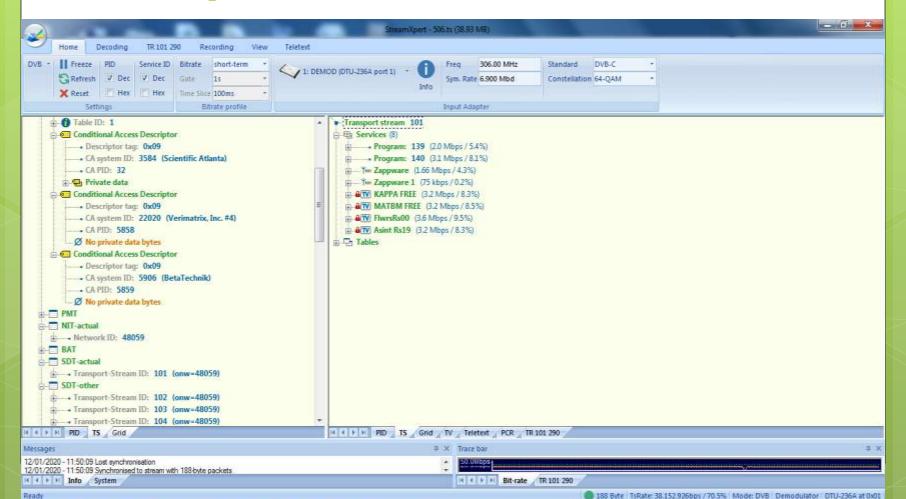
Sample TS Screenshots

Sample тs Screenshots

Key Points to be checked while conducting Audit

- Always check the mux and PSI server configuration in the Headend in order to ensure the following:
    - No of TS configured in Mux w.r.t to no of TS available in the field to verify the existence of any parallel server.
    - Channels configured on dual LCN
    - ECM sharing is allowed or not

- While conducting inspection in the field and Headend always scan the entire channel list for verification of Dual LCN and EPG configured.

- Verify the compliance audit form and subscription audit form submitted by DPO w.r.t to the DAS systems deployed in the Headend.

- Ground sample verification of VC samples and TS shared by broadcasters needs to be carried out carefully while conducting audits.

Audit Report Generation as per audit manual

- The audit report may be prepared as per requirements specified in the audit manual.

- Collect as many evidences and supporting documents during the audit visit and make them part/annexures of the audit report.

- During MSR verification process, select one date from each month to make it an even sample size.

- For VC to VC reconciliation select one random date from each month.

- In case of major observation during technical compliance of any mandatory schedule III requirement always gives opportunity to DPO before writing it as non compliance in audit report.

Thank You!

Questions Please?