



IBF’S RESPONSE TO TRAI’S CONSULTATION PAPER ON FRAMEWORK FOR TECHNICAL COMPLIANCE OF CONDITIONAL ACCESS SYSTEM (CAS) AND SUBSCRIBER MANAGEMENT SYSTEMS (SMS) FOR BROADCASTING & CABLE SERVICES (“CONSULTATION PAPER”)

IBF thanks the Telecom Regulatory Authority of India (“TRAI”) for this opportunity to provide our inputs with respect to laying down of the framework for technical compliance of CAS and SMS.

IBF believes that the inputs provided by us will help TRAI formulate a policy framework enabling protection of content, removal of rampant under-declaration and enhancement of consumer choices and experience.

IBF wishes to highlight that majority of DPOs are still not compliant with the extant regulations and in the absence of any accountability of the DPOs to follow a regimen of audit, and strict compliance with CAS/ SMS technical and operational requirements with corresponding penalties there exists no or very little transparency pertaining to under declaration of the subscriber numbers. There is also an attempt to suppress subscription details by DPOs. IBF is of the view that any sub-standard CAS system fails to make subscribed channels available to the consumer even though payment for the same has been received by the DPO, and provides incorrect information for billing purposes, leading to collection of subscription fees without any records resulting in the risk of un-accounted collections other than leading to piracy of signals, as it is easy to hack or circumvent its security system which in turn leads to compromising the subscriber’s Set Top Box (“STB”) and the subscriber information making the subscriber liable for punishment under cybercrime laws.

The Broadcasters have been bearing the consequences of such non-compliance of the Interconnect Regulations by the DPO and the impact of inadequate provisions to support proper implementation, as the CAS and SMS systems which are essential for content protection and for providing subscriber numbers are under the control of the DPOs. The implementation of a quality standard, and a technical and process framework is essential to deliver the objective of consumer choice, which is the cornerstone of the regulatory framework as structured by TRAI. Under-declaration is not only causing deficiency in servicing the customer, but is responsible



for huge losses to the stakeholders and to the government and equally susceptible to breach, hacking and manipulation. Such unauthorized access to TV channels is in contravention of the guidelines and the regulations laid down by TRAI for the digital addressable regime. Besides, such sub-standard CAS and SMS systems do not allow the subscriber to choose the channels of their choice, thereby adversely impacting the quality of services.

Hence the urgency to create a framework that dwells, spells and resolves these issues and dissuades piracy of content. IBF suggests that the CAS and SMS vendors supplying their systems to the DPOs within India are also made responsible to follow the Schedule III requirements read with the TRAI regulations. If the SMS/ CAS vendor, being one of the stakeholders responsible for delivery of the broadcasting service, is held accountable either directly or by DPO indemnifying and being held responsible for meeting technical and service standards, the same would mitigate quality issues and resolve subscription management.

We suggest that an independent industry autonomous body be set up with the objective of providing the operational framework, observing / adapting global practices and formulating India-related technical standards and be responsible for formulating the prescriptive provisions of schedule III going forward. It would be the remit of such an autonomous body to certify and engage with the technical service providers essential for Digital Addressable regime that do not qualify as “service providers” under the Regulatory statute for e.g. the CAS and SMS vendors and the STB vendors, in administering the techno-operational standards. It would be practical to set up a working group within the stakeholders to work toward the set up of such an autonomous body, as suggested in response to issue no. 5 of this Consultation below.

ISSUE No. 1

List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?



The CAS and SMS deployed by DPOs are required to comply with the requirements laid down in Schedule III of the Interconnect Regulations. Much to the chagrin of our members, it has been observed that the CAS and SMS deployed on ground do not meet the requirements laid down in Schedule III either due to the underhand intention of the DPO or due to the failure to inspect and upgrade the systems appropriately and accordingly.

The said non-compliance of Schedule III by the DPOs diminishes the credibility of the system and gives rise to under-declaration, piracy of signals of TV channels, loss of revenue to the broadcasters and government in the form of taxes and hampers the television viewing experience of the consumer.

Schedule III should be made more compact and watertight, both technically and operationally and the compliance by DPOs should be made more exacting / rigorous which also includes CAS and SMS vendors individually as well as a combined system. Such an effort will ensure in mitigating the impact of sub-standard infrastructure, under-declaration, and eliminate the negative impact of piracy to the entire industry.

Secondly, TRAI should specify the technical features in CAS and SMS systems in details so that DPOs can upgrade their systems accordingly.

An “**Autonomous Body**” to provide the framework for CAS and SMS systems and to oversee strict compliance of the same by DPOs as well as CAS and SMS vendors.

The Autonomous Body to specify the details and upgrade for technical features and operational framework for schedule III, after such Autonomous Body has been formulated.

CAS and SMS vendors should be required register as other service providers and their registration ought to have mandatory pre-conditions such as:



- (a) they will mandatorily register themselves with Autonomous Body and render all such assistances as may be prescribed by TRAI on the lines proposed herein,
- (b) they will ensure that systems supplied by them are always in compliance with provisions of TRAI's Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations 2017 (as amended) ("Interconnection Regulations") (specially Schedule III thereof) and the Telecommunication (Broadcasting and Cable) Services Standards of Quality of Service and Consumer Protection (Addressable Systems) Regulations 2017 (as amended) ("QOS Regulations"),
- (c) they will report agreements with DPOs to TRAI as well as Autonomous Body, and
- (d) they will report all instances of detection of bugs, hacking attempts (successful or not), system breaches, etc. in the system, whether on account of actions / omissions of DPOs or otherwise, to TRAI as well as Autonomous Body without any undue delays.

In view of achieving the digital addressability, a comprehensive list of requirements, including necessary additions and additional features to those specified in current Schedule III of the Interconnect Regulations is proposed for the peruse of the Authority.

Proposed Schedule III as response to Issue 1 of TRAI's CP on CAS & SMS technical framework

Description	Rationale / Requirement
Scope and Scheduling of Audit	
(A) Scope: The annual Audit caused by Distributor shall include the audit to validate compliance with this Schedule and the Subscription Audit, as provided for in these regulations.	Existing clause



<p>(B) Scheduling: The annual Audit as caused by Distributor under regulation 15(1) shall be scheduled in such a manner that there is a gap of at-least six months between the audits of two consecutive calendar years. Further, there should not be a gap of more than 12 (twelve) months between audits of two consecutive calendar years.</p>	<p>Existing clause to be modified</p> <p>The period between two audits has to be reduced from 18 months to 12 months in order to avoid too much gap between audits of two consecutive years.</p>
<p>(C) The Pre-signal Audit The distributor of television channels who is requesting for signals, shall mandatorily provide audit report from an empaneled auditor appointed by the distributor of television channels/broadcaster along with the prescribed application for signals. Only an audit report from such empaneled auditor as provided to Broadcaster and following an Audit conducted as per the prescribed audit manual, by an empaneled auditor, shall be acceptable.</p>	<p>Just self-declaration from DPO is not adequate to confirm that headend is compliant to Schedule III requirement. Third party audit is required to independently verify the compliance status.</p>
<p>Addressable Systems Requirements</p>	
<p>(D) Conditional Access System (CAS) and Subscriber Management System (SMS):</p>	
<p>1. The distributor of television channels shall ensure that the current version of the CAS, in use, do not have any history of hacking. Explanation: A written declaration available with the distributor from the CAS vendor, in this regard, shall be construed as compliance of this requirement.</p>	<p>Existing clause</p>
<p>2. The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.</p>	<p>Existing clause</p>
<p>3. It shall not be possible to alter the data and logs recorded in the CAS and the SMS. Revised: 3. It shall not be possible to alter the data and logs recorded in the CAS and the SMS in any form. The distributor of television channels shall enter into contract with certified CAS and SMS vendors to ensure these transaction logs and data are encrypted and stored on live on-line servers of the CAS and SMS. The logs and data must not be editable in any form. Logs created in CAS and SMS systems shall have hashing or similar mechanism to prove its integrity and to validate whether they have been changed.</p>	<p>Currently, historical transactions logs are exported from CAS and SMS systems to non-live servers and data is not in encrypted form. It is potentially possible to tamper / modify the historical transaction logs. Hence the subscriber reports can be generated with much lower subscriber numbers than the subscriber numbers actually active for the channels. During subscription audits also the tampered logs are made available to the auditors.</p>



	<p>For the sake of analogy, it should be like a flight recorder/ blackbox of an aircraft from which nothing can be deleted, once a log is written nothing could be deleted from this log even by the CAS Vendor itself.</p>
<p>4. 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.</p>	<p>Existing clause</p>
<p>5. The SMS and the CAS should be integrated in such a manner that activation and deactivation of STB happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the SMS and the CAS terminals.</p> <p>Revision: 5. The SMS and the CAS shall be integrated in such a manner that all activation/deactivation of STB/VC, channels, packages, create/modify/delete channels and/or packages etc. shall happen through SMS only.</p> <p>CAS shall always mandatorily be synchronized with SMS and shall execute commands initiated from SMS only through the API. CAS vendor has to certify that no access / login IDs / user interface / application have been provided to the distributor of television channels to execute any commands including but not limited to activation / de-activation, package creation / modification / deletion etc. directly from the CAS by bypassing the SMS.</p>	<p>There are always differences found in STB / VC status (active / de-active) count, in entitlement, etc. This is because of functionality of CAS to directly execute commands of activation / de-activation, package / channel activation / de-activation, etc. bypassing the SMS. This results into STB/ VC being found active in CAS but not active in SMS and hence resulting in under-reporting of subscriber count. DPO use this facility to activate STBs directly from CAS in large numbers which are not reported in SMS. Hence monthly subscriber reports do not capture the accurate subscriber numbers which results in significant revenue leakage.</p>
<p>6. 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.</p>	<p>Existing clause</p>
<p>7. The fingerprinting should not get invalidated by use of any device or software.</p>	<p>Existing clause</p>



8. The CAS and the SMS should be able to activate or deactivate services or STBs of at least Five percent (5%) of the subscriber base of the distributor within 24 hours.	Existing clause
9. The STB and Viewing Card (VC) shall be paired from the SMS to ensure security of the channel.	Existing clause
10. 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.	Existing clause
11. The SMS should be computerized and capable of recording the vital information and data concerning the subscribers such as:	Existing clause
(a) Unique customer identification (ID)	Existing clause
(b) Subscription contract number	Existing clause
(c) Name of the subscriber	Existing clause
(d) Billing address with City and State	Existing clause
(e) Installation address with City and State	Existing clause
(f) Landline telephone number	Existing clause
(g) Mobile telephone number	Existing clause
(h) E-mail address	Existing clause
(i) Channels, bouquets and services subscribed	Existing clause
(j) Unique STB number	Existing clause
(k) Unique VC number.	Existing clause
(l) Unique LCO ID	This is to map the subscriber with LCO and DPO. There are multiple LCOs under a DPO. LCOs form an important link between the DPO and the subscriber and so it is essential that the link is captured on the SMS.
12. The SMS should be capable of:	Existing clause
(a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs.	Existing clause
(b) Locating each and every STB and VC installed.	Existing clause
(c) Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.	Existing clause
13. The SMS should be capable of generating reports, at any desired time about:	Existing clause
(a) The total number of registered subscribers.	Existing clause
(b) The total number of active subscribers.	Existing clause
(c) The total number of temporary suspended subscribers.	Existing clause
(d) The total number of deactivated subscribers.	Existing clause



(e) List of blacklisted STBs in the system.	Existing clause
(f) Channel and bouquet wise monthly subscription report in the prescribed format. Revision: (f) Channel and bouquet wise monthly subscription report (MSR) in the prescribed format. The MSR should be accompanied by monthly subscriber count reports from the CAS and SMS vendors. The CAS and SMS system should automatically generate the MSR as on 7th, 14th, 21st and 28th of each month and thereafter automatically email such system generated reports to broadcasters without manual intervention.	It has been observed that most DPOs provide subscriber reports on letterheads and not system generated reports. This is prone to manipulations and errors. In order to have an independent verification of the MSR, it is essential to have the data from CAS and SMS vendors as supporting documents. The revised MSR format is as provided below.
(g) The names of the channels forming part of each bouquet.	Existing clause
(h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time.	Existing clause
(i) The name of a-la carte channel and bouquet subscribed by a subscriber.	Existing clause
(j) The ageing report for subscription of a particular channel or bouquet.	Existing clause
(k) List of all LCOs who have a contract with the distributor of television channels.	LCOs migrate from one MSO to another MSO without clearing outstanding payments. This clause will assist in tracking movement of LCOs from one MSO to another MSO and recover outstanding/unpaid revenues from the new DPO.
(l) The CAS and SMS system should be capable of generating reports for each and every LCO pertaining to information as defined in a) to j) above.	This is crucial for broadcaster to know package/ala-carte wise choice of subscribers under each LCO and thereby plan their marketing activity. This will attract more subscribers and benefit all stakeholders.
14. The CAS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately 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.	Existing clause



<p>15. 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.</p> <p>Revision: 15. The CAS and SMS 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.</p>	<p>Since all actions are done from SMS, blacklisting need to be initiated from SMS and SMS logs need to keep record of all such blacklisted STBs / VCs so that they cannot be redeployed.</p>
<p>16. It shall be possible to generate the following reports from the logs of the CAS:</p>	<p>Existing clause</p>
<p>(a) STB-VC Pairing / De-Pairing</p>	<p>Existing clause</p>
<p>(b) STB Activation / De-activation</p>	<p>Existing clause</p>
<p>(c) Channels Assignment to STB</p>	<p>Existing clause</p>
<p>(d) Report of the activations or the deactivations of a particular channel for a given period.</p>	<p>Existing clause</p>
<p>17. 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 with the list and retail price of corresponding pay channels and bouquet of pay channels, taxes etc.</p>	<p>Existing clause</p>
<p>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.</p> <p>Revision: 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. Further the CAS and SMS vendor should be equipped to provide software and hardware support to the distributor of television channels installations from their India support teams to ensure the CAS and SMS system with 100% uptime and availability by maintaining main and backup systems.</p>	<p>Many a times DPOs have informed us about non-functioning of CAS and SMS systems and long-time quoted by CAS and SMS vendors to rectify. If CAS is not working, channels are running in unencrypted mode. If SMS system is down then subscription logs are not getting generated. In both cases the subscriber numbers in MSR becomes lower, resulting in revenue leakage. So it is essential for CAS and SMS vendors to provide local hardware and software support for highest system uptime.</p>



<p>19. The distributor of television channels shall declare the details of the CAS and the SMS deployed for distribution of channels. In case of deployment of any additional CAS/SMS, the same should be notified to the broadcasters by the distributor.</p> <p>Revision:</p> <p>19. The distributor of television channels shall declare the details of the CAS and the SMS deployed for distribution of channels. For the deployment of any additional CAS and SMS, the distributor of television channels shall have the additional CAS and SMS audited as per clause (C) of this Schedule and shall inform the broadcaster along with the audit report from the empaneled auditor, within 30 days of deploying any such system. The broadcaster shall have 30 days from the receipt of the report to raise any further objections/concerns.</p> <p>The distributor of television channels shall declare to TRAI the following details which will be published on the website of TRAI and the Autonomous Body: -</p> <ul style="list-style-type: none"> a) Headend hardware and connection schematic with network details b) SMS and CAS systems c) Territory coverage d) List of LCOs. e) Any changes / upgrades to be submitted to TRAI for publication on TRAI's website within 7 days of implementation of the change. 	<p>It has been observed that many DPOs have installed additional CAS /SMS in their headend or other location such as mini headend / standby headend without notifying the same to broadcaster. Hence it is essential to make it mandatory to have either a technical audit prior to the deployment, or else a prior written approval for the system to be installed. By making it mandatory for the DPO to declare the headend details to the Autonomous Body, there are many benefits, including:</p> <ul style="list-style-type: none"> 1) availability of information regarding the up-to-date configuration of DPO's headend including CAS, SMS & MUX etc., 2) DPO's feed coverage area 3) LCO movement from MSO to MSO.
<p>20. Upon deactivation of any subscriber from the SMS, all programme/ services shall be denied to that subscriber.</p>	<p>Existing clause</p>
<p>21. The distributor of television channels shall preserve unedited data of the CAS and the SMS for at least two years.</p>	<p>Existing clause</p>
<p>22. CAS and SMS should be capable of generating historical logs of package creation / modifications / deletion along with date and time stamp. The log files must have continuity of data to ensure no missing information.</p>	<p>It has been observed that during audits DPOs have made alterations in packages. In addition, deliberate attempt is made by certain CAS vendors with the consent of or on instruction of DPOs to not provide package composition and/or package change logs. This leads to inability to ascertain the channel composition of packages for historical period and to validate actual subscriber count. This results in under-declaration.</p>



<p>23. CAS should be capable of detecting clone / duplicate STBs running in the network of the distributor of television channels. Each STB / VC / UA number deployed by distributor of television channels in viewer homes must be unique.</p>	<p>We have come across instances where multiple STBs deployed in viewer homes found to be having same unique ID (UA number). This means that there are hundreds and possibly thousands of STBs in viewer homes that have the same STB ID number. Since SMS and CAS can have only unique STB ID numbers, the hundreds and possibly thousands of additional STBs do not appear in the records of CAS and SMS. This leads to under-reporting of actual subscriber count in the MSR.</p>
<p>24. CAS must comply with CSA-2 or CSA-3 standards of scrambling algorithm and embedded in SoC (“Security on Chip”) in STB. (Existing deployed non-compliant CAS should upgrade to this standard within a period of 6 months).</p>	<p>This is to ensure that CAS operates with highest level of security and integrity to provide high level resistance to hacking and piracy attacks.</p>
<p>25. CAS and SMS must be capable to add / modify new channels / packages within 7 days of Broadcaster and the distributor of television channels executing an agreement for retransmitting signals of channels in ala-carte/ bouquet form.</p>	<p>Currently most DPOs are taking more than one month to add / change package / channel which causes inconvenience to the subscriber and causes huge loss of sales to broadcaster.</p>
<p>26. The logs of the Network Service Manager controlling the compression chain of all encoders and all Multiplexer (“MUX”) and the MUX logs must be maintained with details of audio video PID mapping, service IDs, service names, and all information related to the services and encryption. The distributor of television channels shall provide recording of all the Transport Stream (“TS”) being distributed from its headends on request by the broadcaster.</p>	<p>We have come across DPOs who encrypt / decrypt channels regularly with the intent of under declaring. Further DPOs keep changing LCN, genre ranking without informing broadcaster in violation of terms of agreement. The logs will track the above activities which can be used during audits to verify.</p>
<p>27. Every individual channel should be available only on one unique LCN in the distributor of television channels’ entire network, which includes the LCO networks as well. Channel descriptor should match the channel name. It is not permitted to carry same channel in the entire distributor’s network under another LCN and another channel descriptor by any means of technology.</p>	<p>DPOs and LCOs regularly transmit same channel under more than one LCN. This feature is required to ensure that channel disguise / duplication is not done. Channel disguise / duplication results in under declaration in MSR.</p>



<p>28. Encryption of all channels distributed by the distributor of television channels must be implemented only by the CAS on the MUX and not on any other device of the Headend.</p>	<p>Many DPOs pass the channels through the MUX in unencrypted mode and scrambles the entire stream at the QAM (Modulator) which cannot individually activate / deactivate a channel on the subscriber STBs. This results in under declarations since these channels have no record in the CAS and SMS systems.</p>
<p>29. In case the distributor of television channels deploys Digital Rights Management system (“DRM”) in its IPTV based distribution platform, the DRM should meet all the CAS requirement as per Schedule III including but not limited to maintaining of all transaction logs and anti-piracy features such as overt and covert fingerprinting.</p>	<p>Till specific norms for DRM are released by TRAI, any DRM when used by a DPO in his headend, should be treated at par with CAS i.e. all conditions related to transaction logs, data / fingerprinting etc. should be applicable to the DRM.</p>
<p>30. In case the distributor of television channels has deployed hybrid STBs. The distributor of television should be able to block / remove any piracy related Apps installed in the STB which are used by the subscriber to view broadcaster’s content in unauthorised manner and the broadcaster has brought it to the notice of the distributor of television channels.</p>	<p>In the event DPO has been deactivated by the broadcaster due to breach of contract, the DPOs encourage their subscribers to use piracy apps on their hybrid STBs to access broadcaster channels/ content. This results in huge loss of subscription revenue to broadcaster.</p>
<p>All logs should be stamped with date &time and system should not allow to alter or modify any logs. For the sake of analogy, it should be like a flight recorder/Blackbox of an Aircraft from which nothing can be deleted, once a log is written nothing could be deleted from this log even by the SMS Vendor itself.</p>	
<p>All channels and package configuration detail should be in sync with CAS configuration and mismatch to be detected by the system. The system should do auto reconciliation of channels/ala-carte and all packages with their respective id’s created in SMS with CAS configuration and variance report to be available in system with logs.</p>	



<p>SMS should have complete inventory report with following detail</p> <ul style="list-style-type: none">a. Whitelist detailb. Faulty STB/VC - repairable and beyond repairablec. Warehouse fresh stockd. In stock at LCO ende. Blacklistf. Deployed with activation statusg. Testing/demo location	
<p>The life of EMM keys should not be more than 2 months at any point in time</p>	<p>In many substandard CAS system, it has been observed DPO sends EMM entitlements with expiry period more than 5-10 years. In such scenario DPO can activate boxes directly from SMS with EMM entitlement for 10 years and after that delete the records logs from the database. Since cable is one-way technology the actual EMM resides on the STB and decides the enablement but the CAS shows different status which is not true.</p>
<p>It should be mandatory to send periodic (period should not be greater than 20 days) fresh EMM keys so as to ensure that all old EMM keys get updated at STB end. The STB software should be secure in such a way that no EMM is ever blocked/rejected by STB.</p>	
<p>CAS database should have all reports of whitelist of card/STBs with date and time stamp. CAS vendor should release XML/secure un-editable file of keys/card detail purchased by network and upload in</p>	



<p>CAS server directly and any other way to upload keys/ UA/ VC in CAS database and should capture in logs also.</p>	
<p>Each CAS vendor should declare the database tables which are used to store VC level and Entitlement Level information and database structure of reporting module. There should not be any active unique subscriber outside these tables. Any change in structure of these tables should be approved by agency certifying the CAS. There should not be an option to split CAS database or for creation of more than 1 instance by DPO or vendor. Database to be secure enough to ensure that no one can manipulate the same.</p>	
<p>All logs i.e. user, command and configuration to be in readable, understandable and in analysable format. CAS server (all ECM/ EMM/ any servers installed in field) should capture all command and user level logs with date and time stamp. The logs should contain complete commands including time stamps and type of command and channel/product/package activated or deactivated. The logs should be in a such a format and should contain enough information that Auditor working on the logs should be able to derive all relevant information including channel-wise count of historical period accurately.</p>	<p><i>While conducting audits TRAI empanelled auditors have observed that in a lot of CAS/SMS systems the logs do not contain adequate information and are incomplete which makes the logs of no use in determining accuracy of reports. In some of leading CAS systems also the logs are generated in such a format that they are either not readable, or they are unstructured which restricts analysis on a set of logs for comparison with CAS data.</i></p>



CAS Vendor should maintain a detail of CAS servers authorised by him for each DPO and such data should be provided to TRAI empanelled Auditors when they seek this data. In case any DPO has installed backup, server and connected to main server, CAS system should have some intelligence to track the instances where backup server has been used as main server. All logs of backup server to be maintained by main server also. The CAS should have a mechanism to check and ensure that Main and Backup servers have exactly same VC and Entitlement level information and the servers are synchronised.

CAS Vendors do not maintain information on number of servers allocated/installed for a DPO and related entities, this is sometimes done to under report subscriber base wherein subscribers and logs for a set of subscribers is maintained in a separate server which is hidden and not declared. The hidden/undeclared servers are sometimes purchased and installed by entities which are sister entities of the DPO, but such CAS is integrated with additional MUX installed in remote/mini digital headend. Since the CAS is of same vendor, the same is not easily identifiable as separate CAS in TS recording .In absence of declared table structure Auditor has to rely on whatever data is provided by the DPO/ CAS vendor which results in ineffective audit as subscriber base is systematically hidden by DPO, SMS

(E) Fingerprinting: -

1. The distributor of television channels shall ensure that it has systems, processes and controls in place to run finger printing at regular intervals.	Existing clause
2. The STB should support both visible and covert types of finger printing. Provided that only the STB deployed after coming into effect of these Amendment regulations shall support the covert finger printing.	Existing clause
3. The fingerprinting should not get invalidated by use of any device or software.	Existing clause
4. The finger printing should not be removable by pressing any key on the remote of STB.	Existing clause
5. The finger printing should be on the topmost layer of the video.	Existing clause



6. The finger printing should be such that it can identify the unique STB number or the unique VC number.	Existing clause
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.	Existing clause
8. The location, font colour and background colour of fingerprint should be changeable from head end and should be random on the viewing device.	Existing clause
9. The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the VC.	Existing clause
10. The finger printing should be possible on global as well as on the individual STB basis.	Existing clause
11. The overt finger printing should be displayed by the distributor of television channels without any alteration with regard to the time, location, duration and frequency.	Existing clause
12. Scroll messaging should be only available in the lower part of the screen.	Existing clause
13. The STB should have a provision that finger printing is never disabled.	Existing clause
<p data-bbox="131 1022 1047 1192">14. No watermark or logo of the distributor of television channels should be available on any outputs of the STBs of the distributor of television channels, subject to specifications and terms of an agreement between the broadcaster and the respective distributor of television channels. [Option A]</p> <p data-bbox="131 1224 1047 1425">The watermarking network logo for all pay channels shall be inserted at encoder end only, at the headend of the distributor of television channels, and subject to specifications and terms of an agreement between the broadcaster and the respective distributor of television channels. Any encoder not supporting this logo insertion must be replaced with immediate effect.</p> <p data-bbox="131 1430 1047 1528">Provided that only the encoders deployed after coming into effect of these Amendment regulations shall support watermarking network logo for all pay channels at the encoder end. [Option B]</p>	<p data-bbox="1047 1022 1521 1598">[option A] Existing clause to be amended, to correctly recognise the copyright and property right of the broadcast or TV channel. The current clause incorrectly creates a regulatory basis for the Distributor or network service provider to place its logo on the TV Channel which is a legally protected property of the Broadcaster, while interfering with the content and its enjoyment by way of viewing of the TV channel and the content as created, curated and aggregated for consumers benefit and viewing by the Broadcaster.</p> <p data-bbox="1047 1629 1521 1795">[option B] Inserting the logo at the encoder end is much more robust and is very difficult to remove without disrupting the channel's video.</p>



<p>15. Subject to agreement with the Broadcaster, only one watermark or logo of the distributor of television channels should be available on all or any outputs of the STB of the distributor of television channels.</p>	<p>We have come across instances when one DPO is taken over by another DPO, as a result the STBs of the second DPO displays 2 DPO logos. This is misleading for the subscriber and for anti-piracy identification.</p>
<p>16. It must be made mandatory for all distributors of television channels to schedule and display overt finger printing for a minimum of 2 fingerprints per hour on a 24 x 7 x 365 basis and provide broadcasters with the fingerprint schedule on request.</p>	<p>There have been many instances where DPOs are not triggering fingerprints on regular basis which results in delay in identifying the source of piracy. Continuing piracy results in revenue loss to the broadcaster.</p>
<p>17. The distributor of television channels shall implement Forensic Watermarking / Fingerprinting that is unique per STB for robust identification of an STB. This forensic watermarking insertion must not disrupt / distort the video or audio of the channel or the broadcasters visible or forensic watermarking / fingerprinting.</p>	<p>There have been many instances of DPO STBs not displaying fingerprint due to hacking of CAS / STB. Forensic watermarking is much less susceptible to hacking. Important to have a robust method of identification of STB involved in unauthorized distribution.</p>
<p>(F) Set Top Box (STB): -</p>	
<p>1. All STBs should have a Conditional Access System.</p>	<p>Existing clause</p>
<p>2. The STB should be capable of decrypting the Conditional Access messages inserted by the Head-end</p>	<p>Existing clause</p>
<p>3. The STB should be capable of doing finger printing. The STB should support both Entitlement Control Message (ECM) and Entitlement Management Message based fingerprinting. (EMM)</p>	<p>Existing clause</p>
<p>4. The STB should be individually addressable from the Head-end.</p>	<p>Existing clause</p>
<p>5. The STB should be able to receive messages from the Head-end.</p>	<p>Existing clause</p>
<p>6. The messaging character length should be minimal 120 characters.</p>	<p>Existing clause</p>
<p>7. There should be provision for global messaging, group messaging and the individual STB messaging.</p>	<p>Existing clause</p>
<p>8. The STB should have forced messaging capability including forced finger printing display.</p>	<p>Existing clause</p>
<p>9. The STB must be compliant to the applicable Bureau of Indian Standards.</p>	<p>Existing clause</p>
<p>10. The STBs should be addressable over the air to facilitate OTA software upgrade.</p>	<p>Existing clause</p>



<p>11. The STBs with facilities for recording the programs shall have a copy protection system.</p>	<p>Existing clause</p>
<p>12. The STBs that are transferred from one distributor of television channels to another distributor of television channels by transfer of the LCO, or business acquisition, shall only be deployed by the acquiring distributor of television channels, after;</p> <p>(a) obtaining a NOC from the transferring distributor of television channels to certify that there is no outstanding amount payable by the LCO; and</p> <p>(b) obtaining a certification from the CAS and SMS vendors of the transferring distributor of channels stating that the STBs to be transferred have been relabeled/ reconfigured or revalidated to enable them to be used by the acquiring distributor of television channels.</p>	<p>LCOs migrate from one MSO to another MSO without clearing outstanding payments. This clause will assist in tracking movement of LCOs from one MSO to another MSO and recover outstanding / unpaid revenues from the new DPO. In many instances it has been observed that LCOs re-use the STBs by way of an arrangement with the acquiring DPO and their CAS and SMS vendors. However, the number of STBs may not accurately reflect in the subscriber numbers of the acquiring MSO resulting in under-declaration. The certificate from the CAS and SMS vendors will ensure that all the transferred STBs are accurately reflected in the acquiring DPOs database of subscribers.</p>
<p>13. In STBs with recording facility (Internal / external storage):</p>	
<p>a) Content of the channel should get recorded along with entitlements and should not play out if channel / STB is deactivated due to any reason.</p>	<p>If playout is possible for deactive channel /STB, then there is possibility of misuse of STB for piracy and revenue loss for both DPO and Broadcaster</p>
<p>b) Content should get recorded along with fingerprinting / watermarking / scroll messaging and recorded content should display live FP / scroll message during play out.</p>	<p>This will ensure identifying the STB used for piracy of recorded content.</p>
<p>c) Recorded content should be encrypted and should only play in the STB on which it is recorded. Recorded content should not play out on any other device.</p>	<p>Recorded content cannot be misused for unauthorised distribution / piracy.</p>
<p>13. The distributor of television channels to provide STB and viewing card information in STB user settings menus on a mandatory basis with current date, time, and name/logo of the distributor of television channels as mandatory information at all times.</p>	<p>This information is essential to assist effective subscription audits and anti-piracy ground action. Both these issues lead to loss of revenue for broadcaster.</p>



<p>EMM key should be highly secure and it should not be possible to extract EMM/control word out from STB.</p>	<p>Hacking involves the access to the "Control Word" and its propagation over the internet so that it can be input separately without the VC. The only way to prevent this is to have card less CAS set-top boxes, equipped with a hardware-based root-of-trust. A hardware root-of-trust, provided by platforms such as Crypto Media, offers operators robust security protection with an integrated security core (SOC) which cannot be tampered and the "Control Word" is not under communication outside the security core protected SOC. The advanced embedded type CAS would require the CAS specific secret keys to be fused in the SoC making it secure against hacking.</p>
<p>STB should have chipset level pairing.</p>	
<p>(G) OPERATIONAL FRAMEWORK</p>	
<p>1. The distributor of television channels shall not transmit any transport stream in unencrypted manner, or any blank LCN in the Transport Stream. All channels in the entire network of the distributor of television channels should originate and be in encrypted form, from the distributor of television channels' headend upto the subscriber STB. The distributor of television channels should not permit any of his LCOs to add any channel or content or Transport Stream from the LCO side.</p>	<p>LCOs are adding pay channels from their end many times in unencrypted mode which results in piracy and huge loss of revenue to broadcasters. Apart from this, DPOs are also found to add pay channels on these unencrypted services resulting in piracy and loss of revenue to broadcaster.</p>



<p>2. The distributor of television channels shall provide access to Live CAS and SMS database to the broadcasters on request in a "read only" mode.</p>	<p>This will ensure broadcasters have access to accurate and up to date subscriber information.</p>
<p>3. CAS and SMS should be able to handle, in ala-carte mode, all the channels distributed by the distributor of television channels.</p>	<p>There is a limitation in many current CAS & SMS to provide all channels in ala-carte mode. It is hampering the subscriber to exercise the choice of channels and results in loss of sale for the broadcaster and DPO.</p>
<p>4. DPO shall mandatorily provide program information on the EPG. The EPG banner shall display current date, time, LCN number, name of channel, DPO name or the DPO logo as mandatory information at all times.</p>	<p>In many instances DPOs are not providing program information on EPG which deprives subscribers of upcoming program information. This feature is also required for identifying the source DPO during audits and anti-piracy actions.</p>
<p>5. The Autonomous Body shall publish on its website, information submitted by distributors of television channels on the details of all installed CAS and SMS systems with headend address and date of installation. The Autonomous body shall issue unique CAS and SMS ID for each installation of each CAS and SMS. The distributor of television channels shall ensure that this unique ID is always mandatorily carried in the TS as part of DVB ("Digital Video Broadcasting") information. ** (For Security, where required, this information may be made subject to password protected read-only access by authorized Broadcasters and Distributors)</p>	<p>We have observed that DPOs don't declare all the CAS and SMS installed in their networks. If Autonomous Body provides unique CAS and SMS IDs, it will resolve the issue of 1) Hidden CAS and SMS 2) CAS vendors using same CAS ID for multiple headends in place of unique IDs.</p>
<p>6. CAS and SMS vendors must provide to the Autonomous Body, complete setup details of the CAS and SMS system installed at DPO's headend including all equipment details (CAS EMM server, CAS ECM server, CAS Data server, CAS archive server, Mux 1, Mux 2, Scrambler, CAS Console / application server). The CAS/SMS description, location of the equipment, with description and IP address of each equipment forming the CAS and SMS system respectively.</p>	<p>During compliance and subscription audits it is essential to know details of all components of the CAS and SMS system to ascertain complete logs are obtained of all the CAS and SMS which are installed in the headend. In the absence of this information it is not possible to establish if complete logs were extracted during audits.</p>
<p>7. CAS and SMS vendors should get their system audited/recertified every 6 months by the Autonomous Body to confirm adherence to all security, processes and control requirements as per Schedule III. The</p>	<p>In the current framework of Schedule III, there are many sub-standard / low standard CAS and</p>



<p>CAS and SMS vendors shall provide to the Autonomous Body a self-declaration of compliance every 6 months regarding all CAS and SMS systems deployed by the CAS and SMS vendors respectively.</p>	<p>SMS vendors whose systems are not secure and vulnerable for hacking and tampering of logs and databases. This results in under declaration to broadcasters and not to mention, poor service to subscriber. Therefore, it is essential to have periodic re-certification of the CAS and SMS systems.</p>
<p>8. In case of subscription audit, if the broadcaster is not satisfied with the audit report received from the distributor of television channels then the broadcaster has the right to request the Autonomous Body to seek CAS and SMS vendors to directly make available to concerned broadcaster, complete and accurate CAS and SMS logs, for the period under audit so that the same may be provided by concerned broadcaster to the empaneled auditor appointed by such broadcaster under 15(2) of the Interconnection Regulations. In the alternative, broadcaster should be empowered to call for such information / documents directly.</p>	<p>The CAS and SMS vendors have the knowledge of the actual transaction logs that their systems are generating & storing. Therefore, in case of doubts / dispute it is imperative that the empaneled auditor / concerned broadcaster gets the complete and accurate logs which can be obtained directly or through the Autonomous Body.</p>
<p>9. The distributor of television channels shall use its SMS system to authenticate its subscribers through registered mobile number (RMN) through OTP system before the start of subscription and repeated every 6 months.</p>	<p>Subscriber CAF information is not updated in SMS due to vested interest of the LCO. Hence subscriber information in SMS is not actually reflecting the correct subscriber data. The OTP process will confirm the identity of subscriber. In case the subscriber indulges in piracy the RMN will directly assist in initiating legal action against the subscriber / LCO / DPO.</p>
<p>10. All TS information mandated by DVB standards should be provided fully and accurately by the distributor of television channels in the network. The information should include but not limited to network name, network ID, NIT table with all frequency information etc. The distributor of television channels shall submit this information to Autonomous Body to be displayed on its website.</p>	<p>We have seen that DPOs do not provide this information in their networks. The TS recording without network name, unique ID and frequency range becomes inadequate as evidence for anti-piracy action by broadcasters.</p>



Proposed Changes in the Format for Monthly Subscriber Report (MSR)

A: Monthly subscription reports of channels or bouquets to be provided by a distributor of television channels to a broadcaster.

Reported Month: _____ Year: _____

Date of generation of Report: _____

Date of submission of Report by the DPO: _____

A.1 Monthly subscription of a channel or bouquet shall be arrived at, by averaging the number of subscribers subscribing that channel or bouquet, as the case may be, recorded four times in a month, as provided in table-1 and table-2 respectively. The number of subscribers shall be recorded at any point of time between 19:00 HRS to 23:00 HRS of the day.

Table 1- Monthly subscription for a-la-carte channels

S. No.	Name of the channel	Number of subscribers of the channel on 7th day of the month		Number of subscribers of the channel on 14th day of the month		Number of subscribers of the channel on 21th day of the month		Number of subscribers of the channel on 28th day of the month		Monthly subscription of the channel
		SMS	CAS	SMS	CAS	SMS	CAS	SMS	CAS	
(1)	(2)	(3)		(4)		(5)		(6)		(7)= [(3)+(4)+(5)+(6)]/4
1										
2										

Table 1.1- Monthly subscription for a-la-carte channels per LCO

S. No.	Name of the LCO	Area of operation	Name of the channel	Number of subscribers of the channel on 7th day of the month	Number of subscribers of the channel on 14th day of the month	Number of subscribers of the channel on 21th day of the month	Number of subscribers of the channel on 28th day of the month	Monthly subscription of the Channel
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)= [(5)+(6)+(7)+(8)]/4



				SMS	CAS	SMS	CAS	SMS	CAS	SMS	CAS	
1.												
2.												

Table 2- Monthly subscription for bouquets of pay channels

S. No.	Name of the bouquet	Name of constituent channels of bouquet of the broadcasters	Number of subscribers of the bouquet on 7th day of the month		Number of subscribers of the bouquet on 14th day of the month		Number of subscribers of the bouquet on 21th day of the month		Number of subscribers of the bouquet on 28th day of the month		Monthly subscription of the Bouquet
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
			SMS	CAS	SMS	CAS	SMS	CAS	SMS	CAS	(8)=[(4)+(5)+(6)+(7)]/4

ISSUE No. 2

As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?

IBF wishes to state on record that the CAS and SMS deployed on ground often comply with the requirements laid down in Schedule III only on the day of installation or on the day an audit is conducted. Since these are under the exclusive domain and at the premises of the DPO, the configuration can easily be changed for under-declaration of subscriber base. In this case, Self-certification as provided in the Audit Manual is never commensurate.

It must be made mandatory for the DPO as well as the CAS and SMS vendor to submit all information of the installations at the DPO's headend separately to the Autonomous Body (setting up of such an autonomous body suggested in our response to Issue 5) and the said information should then be displayed on the website of the Autonomous Body. In case the DPOs



believe that the said information should not be publicly available, then all broadcasters who have been granted permission to downlink should be able to view the said details on the website by using user specific log-in id. The CAS and SMS vendors shall mandatorily obtain re-certification of their CAS and SMS systems from the Autonomous Body every 6 months.

The current regulations merely lays down the minimum criteria to be met by the deployed CAS and SMS which ensures all types of CAS and SMS systems to exist in the eco-system. Both DPOs and CAS and SMS vendors should be responsible and accountable for such CAS and SMS systems' as well as performance and system integrity. It is imperative for the DPO to indemnify the systems deployed and the accurate functioning of the same.

In order to address the aforesaid issues, we suggest the following additional compliance measures -

- a) Set up an Autonomous Body: An Autonomous Body be set up to define technical standards and certify the CAS and SMS systems for compliance of requirements laid down in Schedule III. It must be made mandatory for the DPOs as well as the CAS and SMS vendors to submit all information regarding installations at the DPO's headend separately to the Autonomous Body and the said information should then be displayed on the website of the Autonomous Body.
- b) Empanelment of CAS and SMS vendors with the Autonomous Body: As a first requirement to ensure that sub-standard CAS and SMS systems are not deployed, the CAS and SMS vendor must obtain accreditation certificate from the Autonomous Body and be empaneled with the Autonomous Body. This will ensure that only CAS and SMS systems which comply fully with requirements laid down in Schedule III are permitted to be deployed by the DPOs and uniformity across the system.
- c) Pre-signal Audit: At present the Interconnect Regulations allow a DPO seeking signals to submit to the broadcaster a self-declaration stating that the CAS and SMS system deployed by the DPO meets the requirements as specified in the Schedule III. This self-declaration is not enough. An empaneled Auditor should provide an audit report to the broadcasters before the Distributor request for a Signal with an application. The fee and expenses of



such audit or any re-audit required in case discrepancies are found shall be borne by the DPOs. Any deviation should be construed as breach and both DPO and CAS and SMS vendor must be made liable.

- d) **Periodic re-certification of CAS and SMS systems** : The CAS and SMS vendor shall submit a self-declaration certificate on a bi-annual basis to the Autonomous Body for the CAS and SMS system installed at the DPO headend along with complete details of the system, which must comply with all specifications and requirements in Schedule III. This declaration is a confirmation by the CAS and SMS vendors that the systems installed comply with all requirements of Schedule III and an undertaking that if there are any irregularities found during audit the same will be immediately rectified. It shall be the responsibility of the DPO to ensure that their CAS and SMS vendors get their CAS and SMS systems re-certified by the Autonomous Body every 6 months to ensure that the systems are in compliance with the requirements laid down in Schedule III, and as upgraded and published by the Autonomous Body from time to time. In the event, the CAS and SMS systems do not pass the re-certification process, the said CAS and SMS vendors shall within 30 days rectify or upgrade, as necessary, their systems to meet the requirements of schedule III and as published by the Autonomous Body from time to time. The Autonomous Body shall have the power to recommend blacklisting/deleting the list of CAS and SMS vendors who are not compliant. In case of discrepancies found on the ground by broadcasters, the broadcasters shall bring such discrepancies to the notice of the Autonomous Body for dealing with the Vendors, while taking appropriate action against the DPO for ensuring compliance.
- e) **Provision of financial disincentives for non-compliance**: It is essential to provide for financial disincentives and blacklisting, without prejudice to any other / further rights that the broadcaster may have (including the Broadcaster's right to disconnect under the Interconnect Regulations), by provisioning for substantial amounts to be payable as financial disincentives/ penalties by DPOs for non-compliance of Schedule III requirements and discrepancy in meeting the operational framework for implementation of certified CAS and SMS systems. IBF suggests that the defaulting DPOs who are found to be in contravention of the interconnection agreements, Interconnection Regulations (including provisions of Schedule III) and QOS Regulations shall be liable to pay financial disincentives



not less than INR 1 Lakh per day of default and should also be disentitled to seek signals for a period varying from one (1) to five (5) years in terms of TRAI's Interconnection Regulations depending on gravity of default.

- f) **Imposition of penalty for delay in DPO Audit** - In case the DPO fails to cause an audit of its SMS, CAS and other related systems by auditors to verify that the monthly subscription reports made available to the broadcaster are complete, true and accurate as prescribed under Regulation 15 (1) of the Interconnect Regulations, then a penalty of 5% of the monthly revenue of such defaulting DPO shall be payable by the said DPO for each month of delay post the expiry of the 12 month period prescribed under the Interconnect Regulations. At present the financial disincentive i.e. not exceeding INR Two Lakhs (*INR One Thousand per day for default up to 30 days beyond the due date and an additional amount of INR Two Thousand per day in case the default continues beyond 30 days from the due date*), laid down in the Interconnect Regulations is not deterrent enough to ensure compliance for timely audits. Further, in case the DPO fails to cause a Subscription Audit within 6 months post the prescribed due date, the broadcaster should continue to have the right to disconnect signals of such a defaulting DPO.
- g) **Repeat Default by DPO of Schedule III**: If the DPO is found to be in non-compliance of the provisions of the Schedule III twice, then action to be initiated by TRAI against such defaulting DPOs by sending a list of such defaulters to Ministry of Information and Broadcasting ("**MIB**") with recommendation or request for cancellation of licenses of such non-compliant DPOs and their blacklisting for prescribed period of time.
- h) In addition to SMS & CAS other related systems like Multiplexer, DHE & STB are vital component in any digital headend and major role to ensure content security and correct subscription reporting hence Mux and DHE should also include compliance measures and certification from vendors to be made mandatory.

Suggested basic requirements of Multiplexer:

1. Configuration of channel and transport stream as per DVB standard only.



2. Unique ECM PID for each channel and system should not allow to allocate same ECM to more than one channel/service.
 3. Unique access criteria for each channel and system should not allow to allocate same access criteria to more than one channel/service.
 4. Mux should have database and all logs of configurations including scrambling, user level and command level to be captured with date and time stamp.
 5. Unique LCN to be configure for each channel and same LCN should not be configured to more than one channel.
 6. Mux should pass following data in all Transport streams:
 - a. Service provider detail
 - b. LCN detail
 - c. NIT
 7. Mux should not configure any channel or transport stream without content.
 8. MUX should able to detect and disable transmission of any channel without scrambling and encryption from CAS.
- i) In a huge number of instances, entire system of CAS, SMS is bypassed through the mechanism of local Insertion of channels by LCO. DPO configures some channels in TS but does not insert and Audio/Video, the content of which is actually inserted by LCO downstream. In many instances the content such inserted by LCO is Pay Tv content. While the CAS and SMS would have captured such entitlement as local channel or not captured at all as channel is provided in unencrypted manner. In reality the subscribers are enabled with Pay Tv content. Authority should specifically disallow this in the framework so that no local insertion of content by LCO is possible. All content must be inserted by DPO and must be in his control. Even if local content is to be retransmitted, the same should be done by DPO in his main Digital headend in encrypted mode and should not be left to be inserted



by LCO in uncontrolled and unencrypted manner. This current practice of channels which are unencrypted open for local insertion by LCO must be stopped as this is major source of under-reporting and piracy.

ISSUE No. 3

Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?

A robust framework is required to be defined in order to ensure that there is no possibility of manipulation of records and piracy/illegal retransmission of signals of channels by deployment of sub-standard CAS and SMS systems as the same leads to loss of revenue to the operator, broadcaster as well as to the government in form of taxes. Further, such sub-standard CAS and SMS systems do not have an option to back up all the critical data which would render any audit exercise futile.

The framework for CAS and SMS systems to benchmark the minimum requirements must include the technical requirements and specifications as mentioned in the update of Schedule III. Apart from this the technical framework must be strengthened by forming an Autonomous body that will be responsible for defining the framework, Accreditation of the Vendors, ensuring timely upgradation of Schedule III technical specification and operational requirements and continued compliance by the CAS and SMS vendors with the requirements of Schedule III.

ISSUE No. 4

What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?



Consumer choices and viewing preferences is the key. IBF believes that whenever any advancement on the technology and operational front is available, an upgradation invariably should happen. It is submitted that with every new method invented for piracy, an upgrade of the CAS and/or SMS system and/or STB becomes necessary for fixing the origin of piracy.

In the absence of regular updates and upgrades by CAS and SMS vendors, the security of CAS, SMS and STBs will be compromised making the system more vulnerable and prone to piracy of broadcasters' channels resulting in revenue loss for DPOs, broadcasters and the government. This is in keeping with the fact that any unsupported CAS and SMS will be unable to meet the quality of standards as mandated by the regulation.

The safeguards which are necessary to ensure that the consumers and all other stakeholders do not suffer for want of regular upgrade/configuration by CAS and SMS vendors are as follows -

1. Each DPO should always mandatorily have service level agreements (“SLA”) with the CAS and SMS vendor, which include the Vendor's responsibilities to upgrade and maintain systems inter-alia to ensure compliance of stipulations prescribed by TRAI including in Schedule III of Interconnection Regulations.
2. Each DPO should mandatorily renew its agreement with CAS and SMS vendor prior to expiry under written intimation to TRAI and Autonomous Body.
3. CAS and SMS systems should be installed on CAS and SMS vendor recommended servers with proper IT security systems and protocols such as firewalls and other secure features as per the specifications provided by CAS and SMS.
4. CAS, SMS and STBs should be secure and should run with latest security features which makes regular upgradation of system essential.



5. The Autonomous Body shall have the responsibility to review and strengthen the requirements in Schedule III to address novel ways for piracy of TV signals and unauthorized distribution of signals brought to its notice by stakeholders such as but not limited to broadcasters, DPOs and subscribers. Autonomous Body shall maintain a live CAS and SMS testing laboratory for effective compliance checks before issuance of accreditation certificates. These accreditation certificates shall have an expiry date and the CAS and SMS vendors shall ensure that their certificate is always valid when they are conducting any business with any of the DPOs licensed to operate in India.
6. Only the CAS and SMS systems of CAS and SMS vendors empaneled with Autonomous body shall be deployed by DPOs.
7. Regular examination of quality of signals provided to subscribers catered by small DPOs should also be undertaken, to enable improvements in CAS/SMS systems. The Autonomous Body can conduct regular checks of the signal quality delivered to the subscribers at intervals or as requested by a large percentage of subscribers of a particular DPO. The Autonomous Body will give recommendations to TRAI for inclusion in Schedule III, for implementation by the DPO. In case a DPO is unable to rectify the same for more than 6 months, penalties may be applicable till such time they are able to resolve the issue.
8. A CAS and SMS vendor who is unable to provide local technical support and the SLA should be deregistered and disqualified to operate in India and should not be allowed to install any of its systems in India. Such CAS and SMS vendors shall not be empaneled/shall be de-empaneled by the Autonomous Body.



a) Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons thereof. Describe the structure and functioning procedure of such entrusted entity.

AUTONOMOUS BODY FOR TECHNICAL ACCREDITATION, OPERATIONAL FRAMEWORK, MANAGEMENT AND COMPLIANCE

IBF recommends the setting up and creation of an independent, autonomous, neutral body should be set up for defining the framework for CAS and SMS in India. The Autonomous Body may be set up by representatives of Broadcasters (IBF Members), DPOs, CAS and SMS vendors who can be assisted by trained investigators, legal and law enforcement members, cryptography analysts and system / network security auditors). This body shall be entrusted with the task of accreditation, upgradation of specifications with the involvement of technical experts, and through a consultative process with relevant stakeholders defining the framework for CAS and SMS. The technical standards set by the Autonomous Body will be prescriptive for all stakeholders and shall be the source of technical recommendations to the regulatory authorities. The Autonomous Body should take into consideration global best practices and standards while proposing and suggesting the framework/ technical standards for India. The Autonomous Body would be focusing their capacity in solving quality and technical issues for CAS/ SMS framework for television broadcasting services and will perform the following functions:

- a) Prepare an operational framework for specifying the common standards regarding CAS and SMS systems for broadcasting services.
- b) Every 12 months or earlier, if required, furnish various recommendations, resulting from its technical research and testing modalities, on various upgrades and updates that shall be implemented in the CAS, SMS and STBs to make the complete eco system robust.



- c) To come up with new ideas and policy recommendations for TRAI and MIB after studying the practical implementation of CAS and SMS technical and operational factors with ways to resolve on-ground issues, with a focus on the broadcasting services eco system.
- d) Develop expertise to imbibe the latest technologies and results of Research and Development including a possible Block Chain Mechanism.
- e) Provide technical inputs to TRAI and Telecom Disputes Settlement Appellate Tribunal.
- f) To issue accreditation certificates to CAS and SMS Vendors post carrying out testing of the CAS and SMS Systems, and the certificates will be issued with an expiry date of 6 months. Thereafter, it shall be the responsibility of the CAS and SMS vendors to get themselves re-certified from the Autonomous Body every 6 months. The CAS and SMS vendors shall always ensure validity of their certificate.
- g) Manage the empanelment and compliance by the CAS and SMS vendors after issuance of accreditation certificate by the Autonomous Body.
- h) Publish the reports pertaining to certification/re-certification of the CAS and SMS system on its website.
- i) To obtain complete and accurate logs from CAS and SMS vendors for the period under audit at the request of the broadcaster in the event the broadcaster is not satisfied with the audit report received from the DPO. The said logs shall then be provided to the empaneled auditor appointed by the broadcaster for carrying out audits under regulation 15(2) of Interconnection Regulations.
- j) To explore technology supported solutions, including Block Chain solution to ensure that there is complete transparency of the number of subscribers connected to any DPO. This system, if implemented properly, will be very close to eliminating under-declaration faced by the industry. (A suggested approach to the Block Chain



mechanism could be that every transaction that a DPO does with his subscriber will be recorded, transparently available to all stakeholders and will be conducted through the “miners” in the block chain. The movement of a subscriber from one DPO to another will be possible once all dues owed to the DPO are cleared. Without clearing the dues if the LCO / DPO attempts to migrate the subscribers from one DPO to the other, the transaction would not complete due to existing uncleared dues and so on in the Block Chain solution. Eventually all subscribers and the channels subscribed information will be available transparently to all the stakeholders. Information of any DPO who might be delisted would be available transparently as it would not be possible to execute any transaction with that DPO. In short, this mechanism will benefit the entire eco system and all its stakeholders.)

- k) To maintain a list of decommissioned CAS and SMS systems to ensure that such decommissioned CAS and SMS installations are not re-deployed. All CAS and/or SMS vendors who have decommissioned their installations at any DPO shall be accountable to inform the same to the Autonomous Body, which shall inform for the record the Broadcaster and TRAI. On the date of decommissioning the CAS and SMS installation, the list of final subscriber report, logs etc. shall be shared by the Vendor with the Autonomous Body, with a copy to the Broadcaster. If during any Audit, such decommissioned system is found to be operational and not reported to the Autonomous body in advance, it would be a violation of Schedule III and, subject to an opportunity for the Vendor to prove its lack of involvement or wrongful deployment by the DPO, within limited time frame, the following actions shall be taken:
- i. Removal of CAS and SMS vendors from empanelment with the Autonomous Body;
 - ii. The CAS/ SMS vendors shall be placed on the Defaulters list of disqualified CAS and SMS vendors available on the website of the Autonomous Body; and



- iii. Autonomous Body will strongly recommend to the MIB for cancellation of the License of the Distributor of television channel.

b) What should be the mechanism/ structure, so as to ensure that stakeholders engage actively in the decision-making process for making test specifications / procedures? Support your response with any existing model adapted in India or globally.

The Autonomous Body formed for defining the framework for CAS and SMS systems should adopt a consultative approach thereby inviting inputs and innovations from the technical and operational experts available with stakeholders including broadcasters, DPOs, vendors, manufacturers of devices, Research and Development centers and also consider inputs received during such consultation process. This will ensure active participation/involvement of the stakeholders.

Thereafter, the Autonomous Body may lay down the criteria for the technical standards in a transparent manner post consideration of inputs of all the stakeholders.

ISSUE No. 6

- 5. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.**

It is submitted that there is no element of effective deterrence vis-à-vis DPOs who are found in violation of Schedule III and various provisions of the Interconnect Regulations, including audit requirements that are essential for efficient implementation. It is imperative that financial disincentives in the form of appropriate penalties extending upto cancellation of license (*in case of repeated violations*) by MIB be implemented before formulation of any suitable model in order to ensure compliance. Deterrents by their very nature ensure compliance of laid down requirements and frameworks. IBF suggests the Response to Question 2 be considered as proposed deterrents.

- a) Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of**



testing and certification be entrusted with accredited testing labs empaneled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.

It is suggested that the Autonomous Body shall carry out testing and certification of CAS and SMS systems and can also develop the technical expertise for STBs. The Autonomous Body shall be responsible for carrying out extensive review and detailed assessment of the CAS and SMS systems, including by periodic re-certification of the CAS and SMS systems once in 6 months, publishing reports of re-certification on its website, and keeping the Vendors, DPO and broadcasters informed of standards in parallel. Such re-certification of the CAS and SMS systems at regular intervals by the Autonomous Body will ensure compliance of the laid down framework. The verification and/or the recertification process may be conducted by the Autonomous Body with a gap of 6 months.

b) What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation?

Timelines are extremely crucial to deploy effective CAS/SMS systems while recognizing the current status of placement and utilization of systems. The amendment of Schedule III to enable better systems must be affected, at the earliest. In the interim, until the finalization and setting up of the Autonomous Body, the CAS and SMS vendors shall be held responsible for compliance to Schedule III, through the DPO and the SLA between them.

Therefore, a reasonable period, with the availability of technical guidance if needed, should be made, until the designation of the Autonomous Body to take up these activities. All new deployment of systems shall be only in compliance with the Schedule III. A sunset date, i.e. 1 year from the date of establishment of the new framework, shall be laid down for removal of non-compliant CAS and SMS systems.



It shall be the responsibility of all CAS and SMS vendors to get their CAS and SMS systems certified by the Autonomous Body within 4 months from the establishment of the new framework. This will ensure that all the CAS and SMS systems installed/deployed thereafter meet the requirements of the proposed Schedule III.

- c) What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national/ international best practices.**

The Autonomous Body will be responsible for carrying out certification/re-certification of CAS and SMS systems of the CAS and SMS vendors to ensure continued compliance and/or upgradation at any given point in time. Such certification/re-certification reports shall be made available on the website of the Autonomous Body.

During any audit pursuant to the provisions of the Interconnect Regulations, if any DPO is found to be in non-compliance of the provisions of the Schedule III, action shall be initiated by TRAI against such defaulting DPOs by sending a list of such defaulters to MIB with recommendation or request for cancellation of licenses of such non-compliant DPOs. Further, in case of deployment of sub-standard/non-compliant CAS and SMS systems, a list of defaulting CAS and SMS vendors to be published on the websites of the Autonomous Body, TRAI and MIB stating non-compliance of parameters/specifications laid down under Schedule III in the concerned make and model of the CAS and SMS systems deployed by such defaulting CAS and SMS vendors in India. In case of more than 1 such default, such defaulting CAS and SMS vendors should be removed from the Autonomous Body list of empaneled CAS and SMS vendors after 1 event of default. Notwithstanding the action of the Autonomous body, any de-empaneled CAS and SMS vendors shall be required to fulfill their obligations under any existing contracts with DPOs.

To ensure continued compliance need to have following check list for any certification body.



- a. Quarterly or half yearly certificate to be issued to any system.
- b. Independent body to be appointed to validation and compliance check in field and submit report monthly/quarterly.
- c. In case of any new version release by CAS, SMS, Mux systems than old certificate will get invalid and new certification of software version to be get from certification body.
- d. In case any CAS, SMS, MUX, DHE,& STB system gets compromised or hacked or vendor involvement is found in manipulating subscriber reports than that particular vendor to be blacklisted for at least 2 years and all systems deployed in field to be rectified before removal of blacklisting of the vendor apart from a financially penalising the vendor.
- e. Provision of Audit of CAS, SMS, Mux systems by Auditor of repute on Annual basis where Auditor would validate any chosen Product of a vendor installed at DPO premises.

ISSUE No. 7

- 6. Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?**



Once the new framework is established, the same should be made a part of the registration/license conditions to ensure strict compliance by DPOs and any non-compliance may result in penalties or even cancellation of the registration/license. We believe that existing CAS and SMS systems should be mandated to conform to the new framework. A period of four months from the date of establishment of the framework may be provided for such compliance. For the existing and deployed CAS and SMS systems a sunset date i.e. 1 year from the date of establishment of the new framework, shall be laid down for upgradation/replacement with certified CAS and SMS systems. This will ensure level playing field conditions and the achievement of common minimum framework.

ISSUE No. 8

- 7. Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end- consumer experience? Kindly provide detailed comments.**

Standardization and certification of CAS and SMS will prevent revenue leakages in the revenue chain, all stakeholders will get their due revenue, provided the CAS and SMS systems are made tamper-proof and the DPOs do not have the ability of modify these systems to their advantage. The quality of service will improve as with installation of new/upgraded CAS the customers will be able to view channels of their choice thereby improving end-consumer experience. With CAS and SMS systems complying with the requirements laid down in Schedule III, the consumer will not be tied down due to the limitations of the DPOs systems. Further, it will enable complete implementation of the Interconnection Regulations and QOS Regulations issued by TRAI.

ISSUE No. 9

- 8. Any other issue relevant to the present consultation.**



- (a) The Audit Manual should correctly reflect the Operational Framework and requirements of Schedule III. Necessary provision to reflect the position of Pre-Signal audit cannot be circumvented by DPO Self Certification.
- (b) The Regulations must clearly provide for the broadcaster to conduct an audit during the year for the purpose of confirming the continuation of the technical standards.
- (c) TRAI should consider extending the present consultation to Multiplexer & STB also. Before NTO regime most of DPOs were activating all channels/packages on STBs. Post implementation of NTO regulations activation of any ala-carte channel or package happen as per subscriber choice. The role of SMS, CAS and Mux is vital in determining correct Channel wise subscriber count. While TRAI has recognized role of CAS and SMS, the role of Mux is equally important.
