**Response to the Consultation Paper On Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services dated 22nd April 2020**

**Submitted by**
**Rajiv Khattar**
**rajivkhattar@gmail.com**
**Mobile 9899456795**

---

For an effective distribution revenue in industry where each stake holder gets its due and subscriber interest is protect, it is vital that all the elements which ensure that revenues and numbers are accurately captured and reported are effective and truthful.

In India with advent of the DTH and Digital cable the distribution revenues have gradually increased and on average today may be 40% for a Non News Category of Channels and 50 % for the Sports genre and thus a reliable and effective system is important for the protection of the revenue.

Though Conditional Access Systems (CAS), Subscriber Management Systems(SMS) and the Set Top Boxes (STB) play a vital role in ensuring not only the accuracy of the numbers , they also impact quality of service to the consumers, return on investments to the distribution platforms, protect the consumer spend on the hardware.
However Headend ( HE ) is also an important element in the process where the signal originate and are made ready to be distributed and all the commands pass through the same and all the good things in the CAS , SMS, STB are negated and nullified if if the attention is not given to the aspects in the Headend ( HE) , thus it is important to take that also in account

It is an welcome step from TRAI that it has generated a document which will initiate a discussion in this direction and will have long term impact.

It is essential that some baseline guidelines be issued so that the DPO keep those in mind while choosing a conditional access.

To Start with the CAS with advance security and which has chipset pairing should only be allowed, non advance security hence forth may not be permitted and all operators be given time of 6 months from issue of the recommendations to move onto an Advance secure CAS. This will put end to many issues described in the consultation paper. SMS is akin to an accounting and billing software, the criticality of the SMS is the integrity of the data and the time the data is maintained.

Though the development of the specifications is an on going process which needs to keep pace with technology and the business requirements , this process is always on going and thus efforts need to be continuous as one document cannot be called as final one, it may be the final one for the time it is being made.

ISSUES FOR CONSULTATION.

***Q1. 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?***

**Response:**

The Annexure 1 ( Schedule III of Telecommunication ( Broadcasting and Cable ) Services Interconnection

(Addressable Systems) Regulations 2017. of the consultation paper describes the requirement of the CAS and SMS which are required for the purpose of the auditing. However the requirements in the Schedule III and the Audit Manual be synchronized.

The Telecommunication (Broadcasting & Cable ) Service Digital Addressable System Audit Manual dated 8th Nov 2019 ( herein after referred ot the Audit Manual ) released by TRAI is a compressive manual and both the documents which is that Schedule III and the manual be synced into make one .

In any system in a DPO may it be a Digital Cable Network or a DTH network, or HITS network, there is combination of factors that impact the effective, efficient and secure working of the system which minimizes the chances of the misreporting and minimizes the changes.

The implementation and integration of the Headend CAS, SMS and the STB in a proper and effective manner is important and that will yield the desired results. If any of these elements are not addressed we will have a weak link.

In practice the process starts from the selection of the CAS, which has a huge impact in whole value chain. The selection of the CAS decides the selection of SOC or the Chip for the STB, it even sometimes impacts the selection of the Mux for the HE , selection of the SMS as if the SMS has been integrated with a CAS then it is easier and less time consuming to implement in the network. Selection of the CAS also decides if it a secure chip with advance features like chip pairing or keys burnt into the chip are available for it or not.

It has been unfortunate part , the industry in absence of any set norms, scouted for the cheapest solutions and the criteria of selection of the CAS was reverse and was overshadowed by the fact that which CAS provider can provide the cheapest box. This was like putting the cart before the horse as driver of the revenue was the effectiveness of the CAS and not the cost of the STB as the

cost of the STB is one time where as the services are going to be recurring revenue feature and estimated life of the box being 5 years the impact on the revenue is much higher then the cost of the STB which is falling continuously.

There can be many additions to the points listed in the Schedule III , which illustrates the features which are most discussed and gives a visible results, however there more point which need to be considered giving the capability of the system and should be also be a part of the audit manual. Few of the illustrative points will be as

1 What are the warning messages displayed on the screen, as these messages help the remote call center to troubleshoot the issues remotely thus prompting more fast response to the consumer.
2 Does the channels give a preview of the ala carte channels in the consumer list , if yes then how much is the duration of each preview and a consumer can see how many preview in a day.
3 For the cable boxes are the boxes enable to display the unencrypted channel , if yes then it should be treated as an violation. As no unencrypted feed is allowed on the cable networks.
4 Is there a version check on the boxes implemented, for example if boxes are said to be having a software version XX.XX.YY then is there a check enabled that other versions for example XX.XX.ZY cannot work in the system and need to be upgraded, this will check many things, it will also be one of the mechanism that there is no parallel mechanism of the activating boxes which are not in the system.
5 For DTH, are custoemrs able to view the Free to Air Channels in the boxes , this can be done by tuning to the DD freedish boxes.
6 Are the DTH boxes enabled to edit frequencies/satellites to meet the requirements of interoperability.
7 Are there any protections enabled at the output of the box
8 If the box has the recording function , is the recording done in encrypted format, will the recording play with

any STB of the same DPO or with play only with the STB from which it has been recorded.

9 The STB should not play the recorded content if the STB has been deactivated or blacklisted.

10 Does the Box can take a software upgrade or downgrade via an external port on the box or not or does box has an JTEG port.

11 To ensure that all the activation and deactivations are captured appropriately, the CAS data base and SMS data base should be automatically synchronized on two hourly basis.

12 CAS data base should have the capability to record the activations/deactivations/messages sent directly from CAS without receiving the command from SMS, this should be able to be pulled from SAS server.

The set up at the Headend is critical to be understood and need to be understood well. The introduction of a additional mux or an additional port in the mux can facilitate distribution from there can be the most easiest way to bypass all the checks being done.

Another way of bypassing the system is generate two service id or multiple service id for the same channel and show them on different LCNs and activate the second service which is not reflected, each DPO should share its service id's with the corresponding channel in a quarterly report to be uploaded on a website, the Auditors through the rights should be able to download the same and those can be verified on the ground if the service ids are same or different. Even the broadcaster audit team can check on the field via network analyzer if service ids have changed or have remained same or there is an addition or deletion.

On the Technology side, the points raised in the Annexure II of Consultation paper for the Conditional access systems are addressed if the mandate is for an advanced CAS.

1 Control Word Protection is essential and it should always be sent in an encrypted format in ECM.

2 ECM should always be encrypted, else what is the point in having an CAS if the ECM is in clear mode.

3 Hardware Key Ladder is an critical part of the secure box and if the Hardware key ladder is in memory , then it can be extracted, it needs to be in the SOC (Chip ) of the box.

4 Descrambling in the SOC, the more functions are securely done in the SOC the more secure the box becomes and thus cloned boxes can be used to do content redistribution which will harm the Broadcaster and the DPO both. This can be harmful to the consumer also as in case the problem gets rampart the DPO may be forced to change boxes and consumers may have to pay again.

5 Activation , Deactivation of the services is the key to the Digital systems, there exists two types of systems one is never to be deactivated and to be deactivated via a command from the SMS and second is the activated for fixed time and to be deactivated on a particular date. The issue with the first choice is that it keeps the box on and in case of any issue with the SMS or hacking of the boxes where the filtering of the EMM can be done, the box will always remain activated. Though in this the bandwidth is saved as multiple activation commands are not be sent only deactivation command needs to be sent. Second system is that activate a card for a particular period and then those become deactive on a particular date, the load will be staggered as there will be different recharge dates and different cycle end date. This will ensure that a box which has not received the activation command will be not be active and will die itself.

6 Boot Loader is the most critical part of the box, a secure boot loader ensures that no external software can run on top of it and thus is secure enough, Secure boot loaders are must and each booth loader must be signed by the CAS provider, this will ensure that CAS operator is aware of the security of the box and cannot just put the onus on the box vendor, The CAS vendor should issue a certificate every six months that they have randomly selected and tested

the boxes and have found that there is no change in the boot loader of the box which was signed by them.

7 Blacklisting of the STB or the Cards, this is a feature should be there in all CAS and SMS, it is a simple feature that if a Box no or Card no is never to be activated again then a separate data base trigger should be there and if someone tries to activate the card a flag needs to be raised and box not to be activated , in fact normally such boxes are taken out of the databases of the SMS and CAS both, if an operator says my CAS does not allows then it is an malafide objective. If the boxes are not in SMS then they cannot be activated without the direct activation from CAS, which will establish the connivance of the operator in doing so.

8 Direct activation of the boxes from the CAS . There can be an instance where a lot of boxes is activated in CAS and is not activated in the SMS, this is done normally directly from the CAS. It is not practical to block the operations from the CAS as those are required for testing and even in critical times when SMS may have a major issue. The way to counter this is that CAS and SMS should sync themselves every two hours or three hours and any exception report should be generated or a nil report be generated and Auditors should be able to view the same by running the query on the system.

9 Message Que's: Each CAS system has a different way of implementing the same, the developed and matured CAS can be programmed to run the messages in cyclical times and thus the likely hood of message hitting the box is there , in the CAS which are not developed or have not seen a major install base they just send message once and then it is abandoned which makes the chances of it being received minimal, There should be a process to have repetition of the messages esp during the prime time and morning time or during the sporting events , which can be automatic scheduling or manual scheduling.

10 Report formats and Records; The CAS reports can be generated in multiple formats, basis of a pdf report is also an excel or an data base report, thus the

accuracy and authenticity of the report cannot be decided by the format but the way reports are generated. Auditors should run the query before themselves and check the results and same query can be run multiple times to check the data integrity part. The misreporting is not due to the CAS but most of the time intentions; the operator will not like to loose revenue ever.

11 CAS Server Hardware; It is not appropriate to expect that all class of operators will have a similar level of Hardware, it is unrealistic to expect that an operator with 25k or 50k subs even 100k subs will have the same level or Hardware or require same level of Hardware's and data bases. The important here is the integrity of the data bases and the ability to perform the functions.

12 Publication and Sharing of the Service id's : Each channel is defined a service id in CAS, SMS and in Mux, first of all there should be a matching of all the three , secondly it should be shared on a regular basis with all the concerned or may be uploaded on a secure link where the auditors can download the same and check. This can be done without giving notice to the DPO as this will not ask for any confidential information, this can be done instantaneously.

13 Product Information ( Channel Package info) , CAS and SMS work on a product info basis, where each Bouquet of channels is a product. The Product information should be tallied from both the CAS database and the SMS data bases.

14 Reporting from the Mux or the Network management system of the Headend, this should be available on demand and should be preserved in the NMS only

15 For audit the CAS, SMS systems should be able to retain history of the boxes, channels and consumer of a period of minimum 3 years, during the audit a dump of the same can be taken by the auditors to be processed after the query is generated before the auditors.

If the CAS does not performs, as per the requirement in pre signal request stage then those issues should be

pointed then content should not be provided.

Another option of the cross checking of the numbers of the boxes can be done from the GST figures , the GST credit taken for the boxes purchased vis a vis boxes deployed and active can be easily tracked.

It has been observed that all the auditors listed for the audit of the DPO are mostly Finance and accounts related entities and they need to have a strong technical team with them who the experience of understanding the HE, CAS, SMS and STB, they should be having essential equipment's such as network analyzers etc of their own to scan and check the network for essential clues such as if the system is using single CAS in the system or there is another CAS also there, if there is any free to air signal in the network , these are mostly taken on the declaration of the DPO and treated that as final. Even two versions of the same CAS can help in camouflaging the numbers in the network.

The present mechanism of seeking the self declaration for the CAS, SMS and STB from the vendor will not address the concern as vendor will be certifying what the customer is asking for and they have no liability for it.
Thus norms for the vendors be also made strignet so that they are liable , may be saying a wrong reporting will lead to the disqualification of the networks using their products thus for a greater market they will avoid giving wrong declarations.

Many small operators are lured by companies which offer to give them a deal on the CAS and STB, the operators without taking into account long term implications is lured by the deals.

To make the CAS and SMS Companies more accountable, any company which is desirable of selling the products to the DPO , should have an Indian Company of its own. It means it should have an office with the minimum staff of 10 persons on roll ( which should have mix of technical support and development staff so that service can be

provided locally in case of need). The undertaking that they have offices in India to provide services should be coming from both the Principal office as well as the Indian office.

All the transactions of the license fees should be done through the Indian Entity, this will ensure that no fly by night operator works in the nation and providers of the solution are long term solution providers.

It will be worth considering that in addition to the certification to the DPO , should there be a certification be provided to the TRAI by the CAS provider that they have provided solution to which operator, which version and how many boxes keys have been issued. The information on the Keys will be a dynamic one and will have to be updated every time a new set of keys are delivered or activated in the boxes.

This information may be put in the secure domain so that auditors can access the same and then cross check the same with the inventory of the boxes, by adding the stock, active boxes, churned boxes as per the SMS.
This will make the declaration of the boxes to be transparent. This will also help in reduction on the self cloning of the boxes by the DPO if there is such an doubt.

On the STB front also , once the secure CAS or the advanced CAS is implemented , it not only reduces the chances of the hacking/cloning of the boxes.

It is thus suggested that an industry committee be formed and they should look into the revision of the requirements and give the items/points to be added within 2 weeks of the formulation of the committee.

***Q2. 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?***

**Response:**

The Audit in compliance of the Schedule III is more dependent on the self certification by the DPO and CAS providers, the consultation paper on the other hand raises itself many queries on the audit quality and definitely with only handful auditors for the 1000 plus systems it seems a daunting task for the audits to be conducted appropriately.

The current set of Auditors empaneled are having Finance Background with very less technical expertise and experience at their disposal, a set of the requirements for the technical know also needs to be listed for them. The current requirement of 1 year of technical expertise is not sufficient.
The minimum experience criteria should be an experience of 7-10 years in the field of Cable and Broadcasting associated with CAS, SMS and CRM systems and billing systems . The current experience specified of one year is too less . We should understand unlike other branches Broadcasting and Cable is a branch which has no formal institute offering expertise, it is an on the job training and it takes considerable no of years to under the integrated functioning of the HE, CAS, SMS and STB and it can be further complicated by Middleware and other applications on the box

It will help if they can have equipment and the expertise to check the factual situation on the network. It is thus suggested that empaneled auditors should also declare their technical expertise and team which will lead the audit from the Broadcast, CAS, STB and network side.

In order to ensure that a transparent regime is maintained, it should be ensured that no auditor is does the audit of the same DPO for more then 2 years in continuation, it should be eligible to do the audit of the same network again after of the gap of 2 years from the last done audit , plus the

charges of the audit be standardized , this can based on the number of the subscribers and no of Headends to be audited.

***Q3. 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?***

**Response:**

Benchmarking always helps in the process of standardization and development of a robust infrastructure, however considering the network sizes in the country, the basic requirements of the CAS , SMS and STB be laid down, and networks be given the choice how they wish to implement the same

The requirements like Finger Printing have been basic requirement since the days of the analogue conditional access and when the digital networks started coming in force. Thus a network which is not supporting Finger Printing should not be given content, the issue in case can be the requirement of the overt ( visible ) , covert and water marking, a common shoe cannot fit all. The requirements should be as per the network. For example if a network of 25000 subs is asked to implement water marking , it may not be financially viable for all and asking for it may be futile.

We need to understand where all what solution will work. In the closed cable networks which have no IP transits and is confined to a small geographical areas overt ( visible) finger printing can suffice the requirement. Networks which are spread over a large geographical location like a state it may be required to have overt and covert finger printing and water marking.

The networks which are have nation as their operating areas and the boxes can spill over to other markets , water marking can be useful . Normally watermarking solutions

are required when the traditional FP ( Finger printing ) fails which can happen in scenarios where the box is cloned, or the pirate has been able to remove the FP of the operator by using a tool

FP was introduced when it was felt that there will be redistribution piracy on the cable networks ,which is now gone, now the redistribution piracy happens from traditional networks to the OTT platforms or IPTV platforms. For this only FP is not sufficient. For this there needs to be more requirement like Mux available today can give multiple out puts, so all the output logs of the Mux should be recorded and preserved for a period of 3 years and should be available for the audit as and when asked. Operators can be asked to make finger printing more effective by asking them to change the coordinates of appearing on the screen random, from the DPO end the font and color of the FP can be changed, the FP can appear in vertical or horizontal format randomly.

Schedule III should also be categorical that a Finger Printing Schedule of the DPO should be there and should be implemented with the regularity, so that all the boxes in the Universe are able to show the FP of DPO. The Auditor should check that for how many days the FP can be scheduled in the CAS and does the display happen on that schedule , the minimal requirement should be to have the FP schedule stored for 7 days.

It will be good to give basic guidelines and the current set of parameters in the Audit Manual and Schedule III after a synchronized document is made will be an effective and can be expanded after taking inputs from the industry committee.

***Q4. 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?***

**Response**

Consumer is not able to understand the technicalities in the selection of the CAS, SMS, STB or the implementation of the technology, consumer expects that when he pays he get a picture at his house, if he pays for a particular package , he should be able to watch the channels uninterrupted. He should get the number of viewing days he has paid for. Finally his STB should work and it should not fail.

In case a substandard CAS is chosen then it is likely that network may not be able to keep up to the requirements of the business or the regulatory requirements and thus may be required to change the boxes and thus subscriber may be required to pay extra.

Thus it is suggested that there should be some basic mandatory requirements as per the Schedule III updated with the additional requirements after the consultation paper and in addition to same , an implementation of the secure CAS, a secure linkage between the SMS, CAS and Mux be there , the STB should be with advance secure SOC ( Chip) . Going forward there are discussion of the Return Path Data (RPD) thoughts and those will be possible once the secure box is in place.

Each network will have to ensue that the system ( HE, CAM, SMS and STB) it is deploying will meet the requirements of the Schedule III as amended from time to time , without it the content to the network will be stopped if the cure is not done in 60 days. A strict adherence to the same will ensure that the requirements are met with. For the current networks which have deployed the solution which do not meet the requirements may be given 6 months time to ensure they meet the requirements and get the certification from the empaneled auditors.

***Q5. 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.***

***(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.***

**Response:**

International experiences are that Broadcasters and Networks have their own defined parameters and they adhere to the same. From time to time Networks engage third party agencies to study there systems and advise any changes required from the efficienc , accuracy and security point of view.

Even the CAS companies engage third party experts to comment on their product security, the STB manufacturers boxes are tested by CAS companies and third parties for the vulnerability. SMS and CRM solution providers get the quality certifications for the consistency and error in their systems.

Currently the CAS technology providers having user base in India , there are many who have got these certifications done, however there are many who have not got the certifications done, unless they come in the domain of the requirements here which when they have PE ( Permanent Establishment ) here, they cannot be enforced for a regular audit or checks of theirs.

Having a PE in India will ensure that they do not run away when the things do not go their way. They will be liable for the actions at some levels.

The difference between International Scenario and Indian scenario is the network size and the number of the networks.

The whole process as mentioned is the frame work for the system and not just defining the CAS and SMS.

The system is compromised of the Headend (HE), CAS, SMS

and the STB. The consultation paper has not devoted enough attention to the HE implementation which also is big cause of worry as most of the things can go wrong there and whole objective of the transparency is defeated.

The objective seems to be getting hazed by the fact that we are looking at each element separately and treating them as individual standardized product which is not the case in reality.

Each item here is interdependent and the implementation and interface between then is very critical.

In our opinion, the Schedule III and Audit Manual gives a start up point for the requirements , the industry stake holders can jointly add and modify the same and a bi annual meeting of the committee which can have members form all the stake holders, regulator, licensor and may be specialized agencies like BIS, TEC etc so that what is being agreed does not has conflict with their objectives.

For example, BIS can lay standards for the Muxes, STB, Network requirements, signal levels, BER , MER but cannot define how each CAS will integrate with the Mux or the SMS will integrate with the CAS. SMS is an accounting software , it like a simple accounting and billing product , and each has its own features.

Similarly if we are expecting the a CAS vendor will share that how its EMM is built and how it is encrypted or how many milliseconds it is sent on air, how the control word travels then it is not CAS then it is a open system any one will be able hack it. We understand some agencies are trying to wok on it , we need to really look into it , that is that worth it and will solve any practical purpose. As it is highly unlikely that such information will be put in public domain by any cryptography technology provider.

Thus in our view the industry stake holders with few subject matter independent experts , should look at the requirements on the regular basis and keep on updating,
It is must that members keep the legacy systems in place

before recommending any thing and the recommendation be placed for public circulation and comments as the process is currently followed by BIS , TRAI and standard forming bodies.

Each Network has to adhere to the requirements agreed and will have to follow.

**Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.**

***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 empanelled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.***

***(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?***

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

**Response**

The process of implementation , adherence, monitoring and up gradation of the requirements for a HE, CAS, SMS and STB needs to be really kept simple if we do wish to bring in transparency, the more the layers and agencies are involved the more complex and more cumbersome process will become as the onus will be on DPO and all DPO will not have the means to meet the requirements.

Once the stake holders agree to a common frame work, the points should be added to the Schedule III and the Audit manual be updated.

The empanel auditors should ensure that they add the same in their audit report as those added points will form a part of the audit manual.

The provisions should be strictly adhered to and any shortcoming should be given maximum 60 days to be cured. All the RIO have a clause that any variation in the number reported and numbers found in the audit beyond a x% age will be penalized, and these should be strictly followed and published as a deterrent. A repeat offender should loose content for a certain time as agreed by the stakeholders, this may inconvenience the customer but then customer may churn and move to alternative operator or technology.

Once the requirements are given , the DPO should be given 6 months to implement. As there are very less hardware changes being asked , mostly will software implementation and they have to push their technology providers to ensure that conditions are met. Technology providers will be forced to do it as they will be under pressure to loose further business.

The monitoring is done by industry and regulator, the audit defined as per the regulations will be first level of the check and the second level of the check will be periodic audit which broadcasters can ask.
The whole process needs to be industry driven under the watchful guidance of the regulator who holds the power to intervene from time to time.

These points internationally also are dealt by Industry stakeholders. Regulators keep a watch on the proceeds and intervene only when there is a failure of the process.

***Q7. 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?***

**Response**

Once the new framework is established, the existing platforms should be given 6 months time frame to comply with. As mentioned above majority of the items are software driven and can be handled. This will ensure that only serious players will remain and the DPO will force the technology partners to ensure that they comply else they will loose future business.
The points being suggested are good for their business and their investment security and thus should move on with the changes.

***Q8. 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.***

**Response;**

Standardization will bring in the desired level of the transparency in the system which it is required for. Economic efficiency in this business is based on the quantity and quality one wishes to apply to. If there is Middleware implementation in the network then STB specs in terms of memory , power requirement etc may vary and thus the economics may be different from a plain vanilla STB.

A simple question implementation of the 1:1 redundant system or non redundant system on the CAS servers will make the economics different it has no relation to the standardization.

The objective of the process should be that a clear points for the audit manual be brought out, Schedule III should be expanded more, we should get trained manpower for the

audits and compliances and if the compliance is not there it should be reported and the concerned should be penalized either by not providing him the content until the cure happens or imposing financial implications in the RIO with the broadcasters.

***Q9. Any other issue relevant to the present consultation.***

We feel that this effort by the TRAI is commendable however it needs more in depth study , it needs more elements to be brought on the table and debated and industry should forma a consensus amongst itself and come out with the requirements and take the responsibility for implementation and adherence
If we ask the technology providers to provide the detail of their implementation and will like to inspect the same , then trying to reinvent the wheel which will not happen and then whole process will not yield positive result.

One issue which has not been touched anywhere is the audit fees, those needs to be addressed by the regulator as those also need to be standardized to avoid any ambiguity and someone trying to take advantage of the system there.