June 3, 2020

To,
Shri Arvind Kumar Bhardwaj,
Advisor (B&CS)
Telecom Regulatory Authority of India (‘TRAI’)
Mahanagar Doorsanchar Bhawan,
Jawaharlal Lal Nehru Marg,
New Delhi – 110002

Email: advbcs-2@trai.gov.in; jadvisor-bcs@trai.gov.in

Sub.: Consultation Paper dated 22/04/2020 on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services

Dear Sir,

We write to you in response to the Consultation Paper promulgated by TRAI on 22/04/2020 on ‘Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services’ (“Consultation Paper”).

At the outset, we would like to thank TRAI for providing us the opportunity to participate in this consultation process. Please find enclosed herewith our response to the issues raised by the Authority in the Consultation Paper in the interest of various stakeholders and the orderly growth of the Broadcasting Industry.

We hope that our submissions shall be considered favorably by TRAI while evaluating changes to be carried out.

Thanking you,

Yours Sincerely,
For Sony Pictures Networks India Private Limited

Sd/-

Gururaja Rao
Legal Counsel

Encl: Comments on the Consultation paper.

<u>COMMENTS OF SONY PICTURES NETWORKS INDIA PRIVATE LIMITED ("SPNI") TO THE ISSUES RAISED IN THE CONSULTATION PAPER ON FRAMEWORK FOR TECHNICAL COMPLIANCE OF CONDITIONAL ACCESS SYSTEM (CAS) AND SUBSCRIBER MANAGEMENT SYSTEMS (SMS) FOR BROADCASTING & CABLE SERVICES</u>

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?

SPNI response:

i. The content protection is the most important and critical aspect of any Conditional Access System. Creating a secured control word and transmitting it in a secured, encrypted environment to the Set Top Box **("STB")** and decoding it in further secured way defines the robustness of the system. There are few important features of Conditional Access System **("CAS")** and Subscriber Management System **("SMS")** (hereinafter collectively referred to as "**System**"), which are highly concerned with the security of the signals and these need to be standardized.

ii. <u>Entitlement Control Message **("ECM")** & Entitlement Management Message **("EMM")** Encryption:</u>

   Since there are no standards mandated and most of the CAS systems are proprietary in nature, the encryption is not as per international standards. Though few of the international players are maintaining these standards, the same are also not full proof and hack proof.

iii. <u>Control Word:</u>

   Generation of control word should be automatic and it shouldn't be predictable. The frequency in which the control word generates should be unknown. Many sub-standard systems are prone to hacking at this stage also.

iv. <u>Piracy Control features:</u>

Features like fingerprinting and On Screen Display **("OSDs")** to be standardized and complete security of these features to be mandated i.e. it shouldn't be possible to remove/alter the fingerprinting of the box

v. <u>De-scrambling feature in the STB:</u>

The STB is nothing but another CAS, which de-scrambles the incoming signal. Throughout the process in the STB, the signal should remain secured. The integration of CAS in the STB should be standardized to keep signals secure and also regularize the entire process.

vi. <u>Addressability:</u>

The CAS should be capable of addressing each STBs separately, so that cloning and other misuse of signals can be prevented. This can only be achieved with the standardization of CAS software and STB hardware.

vii. <u>CAS & SMS Reports / data base:</u>

All important reports both from CAS and SMS i.e. System should be standardized and the tables should be defined in advance. CAS and SMS manufacturers need to declare the reference data tables of each report to the Trusted Authority and to the auditors. This is important as the root cause of prevailing mistrust originates from the manipulated reports.

viii. On the backdrop of Schedule-III of TRAI Regulations ("**Schedule III**"), which gives a macro guideline on the technical requirements and the compliance features of CAS & SMS, though it touches upon the general requirements of the System, but it is not enough to standardize the CAS and SMS as per the Digital Video Broadcasting ("DVB") standards.

ix. There are various clauses in Schedule-III, which needs to be standardized with clear technically supported features/ documentation by Trusted Authority (Trusted Authority can be a committee of experts (Technical) from all the stakeholders or alternatively TRAI can appoint Department of Electronics and Information Technology as the Trusted Authority)

x. Here are few instances listed our from Schedule III, which according to us are merely an “ instructions to follow”, but without any specified technical standards to CAS/SMS and Original Equipment Manufacturer (“**OEM**”).

- The distributor of television channels shall ensure that the current version of 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.

  As explained above in the Schedule III, the mere submission of self-declaration on vendor’s letterhead doesn’t make any difference. We have seen the declarations are being printed, signed, stamped and submitted to the auditors. This process doesn’t give any guarantee/confirmation that the System has not been hacked or is not capable of being hacked.

  To make it more effective and useful, Trusted Authority or Industry Licensing Authority (ILA) should come out with a periodical list of all CAS versions giving the status of their software, whether the System has got hacked somewhere in the world, if yes then what remedial action the OEM has taken to minimize the impact. This will ensure the security of the content being transmitted. Also, this step will make CAS vendor/ OEM answerable to the Authority as well as to the Distribution Platform Operator (“**DPO**”) and the Broadcasters.

- It shall not be possible to alter the data and logs recorded in the CAS and the SMS.

  Explanation: There are many CAS and SMS/Systems in use today with least importance given to the security of data. Such Systems don’t even care for their own logs safety. We have witnessed couple of vendors having even altered the logs of events (activation, de-activation dates, time etc.). If the System installed is configured, tested and validated by the Trusted Authority or ILA like authority such incidents wont happen.

To make CAS/SMS data and logs untouched and un-altered, it requires robust system level, chip level security measures. These standards are already in force in several European and American countries.

Need to implement robust technical standards framework in CAS and SMS. Prior to the rollout, CAS/SMS vendors need to get their systems validated and certified by the requisite agencies who are specially authorized by the Authority in this regard. Thus, the standardization of CAS and SMS /ystems can remove the trust deficit prevailing among the stakeholders.

- The fingerprinting should not get invalidated by use of any device or software

  Explanation: Piracy control is an important aspect of the addressable systems. There are many methods through which we can control illegal transmission of signals. Fingerprinting mechanism is one of them and widely used as the effective method.

  Many CAS in use today have the feature of fingerprinting for the namesake. This feature can be defeated by a small piece of software by a pirate. Many times, these CAS don't display fingerprints at all, even after scheduling them. So, all these anti-piracy features in the Schedule III have mainly become a procedural tick mark for many of these vendors as there are no standards set in the industry.

  Therefore, there is a need that the Authority must implement strict technical specifications standards for piracy controlling features at the design level itself.

- The STB and Viewing Card (VC) shall be paired from the SMS to ensure security of the channel.

  Explanation: Both CAS and SMS/Systems should have industry standards backed by Regulation and designed by technical experts for all the features including piracy control.

- 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.

  Explanation: Often we have witnessed that CAS and SMS are not able to generate basic reports such as total number of subscribers active as on given date, package edit logs etc. This is due to the lack of initial technical parameters set out for both CAS and SMS.

  Currently vendors come out with the CAS and SMS as per Schedule III, which is a macro guideline given on the general features and not dealt with the standard technical specifications. They use this as the gateway to get their products into the market without any standards. This is basically creating a mistrust among the stakeholders as these types of substandard software/ Systems allow the user (vendor/DPO) to manipulate the numbers/ reports etc.

- The CAS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the CAS including but not limited to activation and deactivation commands issued by the SMS.

  Explanation: As explained above, the Schedule III features give a general type user guide manual/instruction and doesn't mandate any technical standards to be followed by vendors.

  For e.g. Schedule III recommends CAS to be independently capable of generating, recording and maintaining logs- "capability to generate, record or maintain logs" and possess technical specifications detailing- what type of logs, how those logs are being generated, what precautions the OEMs should take while designing, which are the tables the said software should refer to, can the user alter the logs, what and which are the restrictions built in the Systems etc. As of now, there are none of the above standards specified. So, it becomes difficult for the auditors to audit the System in absence of such technical standardization.

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?

SPNI response:

We should note that, audit manual was drafted and based primarily on Schedule III. The entire audit manual revolves around the audit scope and how the auditor must perform audit as per the features given in the Schedule III. This basically means that the auditor is simply checking the features as given in the user manual.

The basic problem here is there are no technical standards are set for an important piece of Digital Addressable System ("DAS"), i.e. CAS and SMS.

Let's understand the above with an example by taking the relevant clause from Schedule III:

The SMS should be capable of generating reports, at any desired time about:

(a) The total number of registered subscribers.

(b) The total number of active subscribers.

(c) The total number of temporary suspended subscribers.

(d) The total number of deactivated subscribers.

(e) List of blacklisted STBs in the system.

(f) Channel and bouquet wise monthly subscription report in the prescribed format.

(g) The names of the channels forming part of each bouquet.

(h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time.

(i) The name of a-la carte channel and bouquet subscribed by a

subscriber.

(j) *The ageing report for subscription of a particular channel or bouquet*.

The above clause doesn't say anything about how the SMS server software refers to the data involved. When the auditor/ user extracts a report for total number of active subscribers, which are the tables in the software being referred, is this given server a real one or a proxy one and are these set of queries, report formats vulnerable to manipulation etc. are unknown and can't be judged. The auditor is completely dependent on the operator/ vendor for all this information. There are no in-built precautionary guidelines meant for OEMs. Vendors and Operators on their own whims and fancies can alter the reports and present their versions both in CAS and SMS.

We should keep in mind that, all these reports which are listed in Schedule III are front end report formats. The CAS/ SMS Vendors design these reports based on the clauses and the requirements of the stakeholders. Any vendor can manipulate these reports by referring to a partial data base without the knowledge of broadcasters or even the Government. Even in the current audit procedure, one can't find out the tables referred as they deny the access to the back-end software by giving the excuses of data security.

This gap can be eliminated if these Systems are subjected to Trusted Authority/ILA before rolling out in the market with a proper industry standardization.

This manipulation is rampant today even in the so called "standardized" CAS / SMS in India. There are more than 90% of CAS and SMS/ Systems in use today which are basic ones and they do not even have any security features to safeguard data. Also, they are very "user friendly" for manipulators.

So, the mere certification from CAS/SMS vendors on compliance is not enough. Self-declaration doesn't work effectively in this type of environment. As stated in question 1, the Authority/Regulator should think of establishing a technical committee/Trusted Authority/ Industry Licensing Authority to approve all the systems including CAS and SMS and related head-end equipment. The Authority should lay down the technical specifications of such Systems starting from chip level to the robustness of the software used. It should become the industry standard through which all the wrong doings can be eliminated.

The standardization procedure can be carried out with industry technical experts, Department of Electronics and Information Technology and any other competitive agencies.

Further, in case the DPO fails to cause an audit of its SMS, CAS and other related Systems by one the empaneled auditors to verify that the monthly subscription reports made available to the broadcaster are correct as per the Regulations the Authority should look at enhancing the penalty amount, which has been presently prescribed for the said non-compliance. Also in case a DPO who is repeatedly found to be in non-compliance of the Regulations, the Authority should also escalate the issue with the Ministry of Information and Broadcasting with a request to have their DAS license cancelled.

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?

SPNI response:

Yes, we are of the opinion that there is an urgent need to define a framework for CAS and SMS/Systems to benchmark the requirements of the Systems due to the reasons as stated in the foregoing clauses. Such new frameworks should be effective for all the existing systems as well. We firmly believe that this would also help protection of content, removal of rampant piracy and under-declaration of subscriber base and enhancement of consumer choices and experience thereby benefiting all the stakeholders. Hence the urgency to create a framework that would look at resolving the issues as raised herein. Further the CAS and SMS vendors supplying their systems to the DPOs within India should also be mandated to follow the Schedule III requirements read with the TRAI regulations strictly and they should be made accountable for the same.

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?

SPNI response:

The proposed new framework exercise is towards standardization of CAS and SMS/Systems. In line with the European standards like European Telecommunication Standard Institution ("**ETSI**") or Japanese standards like Association of Radio Industries and Business ("**ARIB**"), product level technical standardization is required. Based on these standards, all CAS/SMS, OEMs should design their products. For Systems already existing in the market, upgrades can be done with the consent from the Trusted Authority, with minimal discomfort to all the stakeholders.

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.

SPNI response:

We propose an independent industry body comprising mainly the technical members from all the stakeholders including Government, Broadcasters, DPO and the OEMs (CAS/SMS) to define a framework for CAS and SMS in India.

The task of this body should be to primarily define and set the framework for CAS and SMS/Systems, which should be a benchmark for future deployments.

This industry body, which can be termed as the Trusted Authority or Industry Licensing Authority or by any other suitable name.

This group should consist of following professionals-

- Subject experts from Ministry of Electronics and Information Technology / Department of Electronics and Information Technology, Bureau of Indian Standards ("**BIS**")
- System experts from OEMs (CAS/SMS)
- Technical representation from members of the Indian Broadcasting Foundation
- Technical representation from DPO bodies like All India Digital Cable Federation ("**AIDCF**") etc.
- Designated officials from the Authority/Regulator

This core group/ Authority will be recognized by the Government and the industry. The standards as may be defined by this group can thereafter be implemented/executed through certification agencies like BIS, STQC Directorate, QCI etc. Such assessment may include product testing, product certification and conformity to quality management systems etc.

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.

SPNI response:

In the process of defining specification/ standards by the core group, inclusion of all stakeholders itself gives a positive sign to actively involve in decision making exercise.

Following procedure/ mechanism will further smoothen the engagement-

- Government regulation mandating the standardization of CAS and SMS/ Systems
- Educate the existing DPOs whose Systems are substandard and needs an upgrade

- OEMs and vendors need to communicate the approximate cost estimation required to upgrade and also the time required to make suitable upgradation

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.

SPNI response:

Once the technical framework for CAS & SMS is developed and standards are in place, the testing and certification (execution of new standards in existing systems) must start. To make this more effective, robust and practical, following methods need to be adopted.

- This execution body or Licensing Authority will test and certify the systems as per the standard framework set by the core group.
- This testing and certification task should be entrusted to Government controlled accredited testing labs empaneled by industry experts.
- By appointing such an Authority (with Government, industry and standards experts), impartial certification can be achieved.
- Eligible OEMs will get their Systems approved and the substandard Systems will get filtered out

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?
SPNI response:

Any change in the status quo would bring disruptions and problems. To minimize the impact of implementation of new framework, following precautions should be undertaken.

- Set a time frame for implementation
- Inform all the stakeholders about the upcoming implementation of new framework, which will enhance the security and quality of the systems
- A strict monitoring by the authorities should be there on vendors and DPOs while implementing the new framework
- Chances of vendors asking for an exorbitant amount for upgradation from DPOs
- Authorities should mandate the new framework without any additional burden on the consumer. Government can also provide tax benefits to DPOs to the extent of the cost incurred in upgrading SMS and CAS and possibly STBs while implementing the new framework

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

SPNI response:

After the successful testing, certification and accreditation, the System gets rolled out. To keep this compliance going without any interruption even after version changes or software upgrades, the OEMs / vendors should ensure that the upgraded version or the new add-ons should be tested and certified through the Trusted Authority prior to the upgradation. This will ensure the continued compliance.

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?

SPNI response:

Once we have a new framework in place to test, certify and accredit a product/system, following mechanism can be introduced to ensure all the CAS/SMS OEMs/ vendors comply with the specifications:

- All the important parts/ software pieces to be tested as per the standards designed. Please note that a CAS is a set of software and hardware combined together gives the content security, so it is utmost important to test it’s primary components for better and secured performance For e.g.
    - Vital systems of CAS like ECM, EMM encryption, Control Word (CW) safety must be tested and certified
    - Typical and critical logs creation and logs recording must be tested and certified
    - De-scrambling module (CA module to be embedded on STB) to be tested for its security
    - If the CAS is smart card based, then to be tested for content security
    - If it is System on Chip (“SOC”), then chip level security tests to be done.
    - All the important (mandatory) reports programming must be tamper proof. No one should be able to alter the tables without leaving the logs.

- The above checks should be performed with SMS too

Existing and already deployed CAS and SMS Systems also should be mandated to conform with new framework within a stipulated timeline. Once these new frameworks are in force, the transition to the new Systems should be completed within say 9 to 12 months’ timeframe.

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.

SPNI response:

- Yes, we earnestly think that the standardization and certification of CAS and SMS/Systems will bring a lot of new positive changes in the industry.
- Screening, testing and certification of new CAS and SMS/Systems at entry level itself filters out the substandard products from the market
- Tamperproof, robust systems can bring in trust between the stakeholders
- Once it is proved that the Systems are tamperproof and reports are genuine naturally all the stake holders can be in advantageous position
- Control on the revenue pilferage for the relevant stakeholders including the Government
- Consumer can have uninterrupted services with reliable Systems.

We also firmly believe that there should be some penal provisions imposed on the DPOs who are in non-compliance with the new framework as a deterrent measure. In addition to the rights granted to the Broadcasters to disconnect the signals of its channels under the extant TRAI Regulations, it would help if there are additional penal consequences imposed including but not limited to debarring the concerned non-compliant DPOs from receiving the signals of the Broadcasters for a certain number of years in future (say 1 to 2 years). Such stringent penal provisions would ensure that the DPOs are serious in implementation of their Systems in accordance with the Regulations and guidelines laid down by the Authority.

Q9. Any other issue relevant to the present consultation

We hereby wish to humbly submit that there are still substantial number of DPOs whose SMS and CAS may not be compliant with the extant TRAI regulations and in the absence of any serious accountability of the DPOs to follow a regimen of audit, and strict compliance with CAS/ SMS technical and operational requirements with corresponding penalties there would be no transparency and high chances of under declaration of the subscriber numbers. Presently, the Regulations allows a DPO seeking signals to submit to the broadcaster a self-declaration stating that their CAS and SMS system deployed by the DPO meets the requirements as specified in the Schedule III. We sincerely believe that this self-declaration is not enough. It should be made mandatory for the DPO to get its Systems audited by an empanelled Auditor and provide an audit report to the broadcasters before the Broadcaster proceeds to provide its signals to the said DPO upon its request.

You would appreciate that any sub-standard CAS system would not only aide piracy but would also fail to make subscribed channels available to the consumer even though payment for the same may have been received by the DPOs. Further it would also provide incorrect information for billing purposes, leading issues pertaining to collection of subscription fees. Needless to add it would be easy to hack or circumvent the security system of such sub-standard systems, which in turn would lead to compromising the STBs. Hence it is very critical for the Authority to consider the suggestions provided herein below. We would also request that the Regulatory should adopt an integrated approach and any changes / regulations / directions, which is proposed to be brought about by the Authority including in the matter under consideration in the present Consultation Paper should be dovetailed with other initiatives for the sector by DeITY, Ministry of Commerce, MIB and others giving adequate time for transition that will benefit Indian Manufacturers.

In light of the concerns as elucidated above, we humbly request your goodself to kindly look into our aforesaid suggestions and take the same into consideration while evaluating changes to be carried out.