TIMES NETWORK'S COMMENTS ON

CONSULTATION PAPER

ON

FRAMEWORK FOR TECHNICAL COMPLIANCE OF CONDITIONAL ACCESS SYSTEM (CAS) AND SUBSCRIBER MANAGEMENT SYSTEM (SMS) FOR BROADCASTING & CABLE SERVICES

ISSUED BY TELECOM REGULATORY AUTHORITY OF INDIA ON

22ND APRIL 2020

TIMES NETWORK

NOW OR NOTHING

DATE OF SUBMISSION : JUNE 3, '20

(Without Prejudice)

Introduction:

The Digital Addressable System (DAS) offers various advantages to all the stakeholders in the broadcasting value chain vis a vis the analogue system which was prevalent earlier. DAS has resulted in high channel carrying capacity, addressability and transparency. From the consumer's perspective, DAS offers better quality for all channels, selection of channels as per choice of the customer, value added services, convenience of EPG and overall a much better viewing experience.

CAS and SMS are pivots of the DAS and are responsible for delivery of the content in a secured manner to the authorized subscribers. A broadcaster supplies an IRD to a DPO to receive and decrypt the encrypted signals of its channels. The DPO receives the channel authorized by the broadcaster. The decrypted signals of the channel are then encrypted again by the DPO and distributed either directly or through its linked LCOs to its subscribers.

The channel is authorized to be viewed by a subscriber through the SMS and CAS. The SMS communicates with the DPO's CAS to activate the channel on a subscriber's STB. This is done to prevent piracy of the broadcaster's channel. Piracy directly affects a broadcaster's revenue and his ability to invest in production and acquisition of content.

In spite of having CAS and SMS systems, there are various ways through which there is unauthorized usage of the broadcasters content by means of malfunctioning of the SMS and encryption system, re-transmission of pay channel in analogue mode, use of unencrypted feed, multiple SMS and CAS systems, unauthorized sharing of broadcasters signals, using main head-end and multiple mini head-ends to under-report subscriber numbers etc.

CAS and SMS are also susceptible to security threats including network/ software attacks, control hijacks, reverse engineering, malware etc which, in-turn results in content theft/ piracy, degraded quality of service to consumers, financial loss, integrity violation of data etc.

We feel that most DPOs are still not compliant with the extant regulations and there is no strict compliance with CAS/ SMS technical and operational requirements as stipulated in the Interconnection Regulations. Further there is lack of penal provisions in the Regulations if there is violation of the standards by the DPOs. Hence there is very less transparency which results into under declaration of the subscriber numbers. The subscription details are also not properly and fully reported by DPOs. Any sub-standard CAS/SMS system damages the entire ecosystem and defeats the main objective of digitization of Cable services in the country.

The CAS and SMS systems are essential for providing subscriber numbers which is the basis for arriving at the revenue share between broadcaster and DPOs. There are possibilities for ground level tampering / manipulation due to various reasons such as lack of enforcement provisions in the Regulations for the compliance, non-application of the standards to the CAS/SMS vendors. Even the audit recourse which is provided to broadcaster is not fool-proof and the DPOs purposely delays the audit and many a times the broadcaster has to approach Hon'ble TDSAT for getting the audit conducted. The Broadcasters have to bear the consequences of such non-compliance of the standards for CAS/SMS system. The proper implementation of a technical standard and process framework is essential for proper functioning of the new regulatory regime. 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 thereby also infringing on the copyrights of the content providers. Any such unauthorized access to TV channels is in contravention of the MIB Guidelines and the TRAI Regulations.

Thus, in our opinion the deployment of CAS/ SMS systems may be based on a standardized technical compliance framework, subject to tests and certifications and enabling provisions for strict compliance and enforcement by all concerned including the CAS/SMS vendors. The generic framework given under Schedule III of the Interconnection Regulations, 2017 and the Audit Manual, as prescribed by the Authority should be further strengthened with technical standards and requirements so that the chances of piracy and under-declaration of subscribers are reduced to a great extent.

The framework for technical compliance for CAS and SMS also need to look into safe and tight integration of CAS, SMS and other related systems so as to ensure that the integrated system is not susceptible to the evils of hacking / piracy and that the Broadcaster's content is secured thoroughly in the entire distribution chain.

Further there is need to have a strong and independent, autonomous institutional machinery to aid and support CAS and SMS smooth functioning and the registration process for the CAS and SMS vendors including the foreign players.

With the above premise, we hereby submit our question wise response to the CP as below:

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?

Comments :-

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 are as follows:

Under Interconnection Regulations, 2017:
i. Ensuring usage of current version of CAS – Scrambling; Encryption/ Decryption
ii. Capability of SMS to independently generate record and maintain logs; execute activation and deactivation commands.
iii. Generation of unalterable data and logs by CAS & SMS
iv. All activation and deactivation of STBs to be done with the commands of the SMS.
v. Capability of CAS to upgrade STBs over-the-air
vi. Usage of fingerprinting and watermarking techniques
vii. Pairing of Set Top Box and Viewing Card to ensure security of channel
viii. Capability of CAS to tag and blacklist VC/ STB nos. to check for piracy and thus discourage their re-deployment

Others:
i. Use of standardized microcontrollers in the CAS/ SMS systems, which act as a shield against tampering and cyber-attacks. The standardized microcontrollers are characterised with security features like Advanced Encryption Standards (AES), Cyclic Redundancy Checks (CRC), Memory Protection Units (MPU) Automatic commands on subscription, certification of CAS-SMS systems.

However, it shall be ensured that there are adequate provisions made in the Regulations which enforce the prescribed standards to have meaningful and effective implementation.

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?

Comments :-

From Table 1 of the Consultation Paper, it can be clearly observed that the CA Systems currently deployed in India differ in the type of embedded systems and other technical parameters used by them. As rightly pointed out by the Authority, the CA Systems which do not use the advanced embedded security and deploy sub-standard solutions can be vulnerable to hacking, thereby putting content security at risk. This necessitates the need to first standardize the framework for embedded systems as well as other technical parameters in CA Systems, which may be used by the DPOs. The standardized framework would contain the threshold parameters for all the CAS service providers, based on which they would proceed to design/ upgrade their systems and get necessary testing and certification by an Autonomous Body to be set up.

Similarly, the Authority, in Table 2 of the CP has highlighted the different types of Subscriber Management System deployed by the DPOs. It has further stated that the listed SMS have varying capabilities without any direct linkage to the CASs deployed.

Thus, the possibility of a common framework for an integrated CAS and SMS service needs to be worked upon, which may further make it easier to streamline the framework for related components like System on Chip (SoC), fingerprinting, On – Screen Displays (OSD), which otherwise have to be dependent on the type of CAS/ SMS facility being used.

The foremost intention of this exercise should be to ensure the uncompromised security of the CAS, SMS and the entire related addressable system and its insusceptibility to piracy/ hacking.

We suggest that the CAS / SMS vendor should be registered in India with the Institutional Authority like an Autonomous Entity envisaged herein below. This will ensure that there are no sub-standard systems and software which can be deployed or used by the service providers. This will also ensure that there is proper update/ upgrade of the systems from time to time as and when the same becomes available. It is an established fact that the use of the outdated version of such systems are more prone to hacking and manipulation.

As far as the compliance with the parameters listed in Schedule III of the Interconnection Regulations, 2017, as amended till date is concerned, the certificate from Autonomous Body which has done the testing and certification of the CAS/ SMS systems of the vendors registered with it shall be given. Further, there shall be an annual re-validation of the Certificates issued to such vendors / systems.

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?

Comments :-

We feel that there is a need to define a standardized technical framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India. The deployment of CAS/ SMS systems is suggested to be based on advanced embedded system backed by mandatory tests and necessary certifications using defined standards. CAS must comply with CSA-2 or CSA-3 standards of scrambling algorithm and embedded in SoC ("Security on Chip") in STB. The standards should be made keeping in mind that these are at par with global standards and are also useful from middleware perspective. There may be a specific SOC for CAS which will minimise the chances of hacking. It should be endeavoured that no sub-standard systems can be deployed. As regards existing deployed non-compliant CAS, they should upgrade to this standard within a period of 12 months from date of implementation of new standards with a view to give sufficient time for migration. This will give added protection against hacking and piracy.

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?

Comments :-

Having once installed a standard system cannot serve the purpose forever as the technology changes over a period of time and many new methods of hacking or manipulation of the system comes into play. Hence any good system needs to update and upgrade itself to keep it in consonance with changing technological landscape. Hence, the systems to be deployed should be subject to regular upgrade by CAS and SMS vendors. Hence a yearly re-validation and re-certification by the Autonomous Body may be made mandatory in this regard. This will also minimize the requirement on the part of the broadcasters to cause the audits of the DPOs systems. Further, CAS, SMS and STBs should be secure and should run with latest security features which requires regular upgradation of system essential. The CAS and SMS vendor who is unable to provide local technical support and the required service levels should be disqualified to operate in India and should not be allowed to install any of its systems in India.

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.

Comments :-

As CAS and SMS are pivotal for DAS eco-system and are responsible for delivery of the content in a secure and encrypted manner only to the authorized subscribers, it is important that the standards being set for CAS and SMS are quite adequate to ward off the various risks. We feel that 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, DPOs, CAS and SMS vendors, technology vendors, manufacturer or importers of devices, representatives of R&D Centres, members of regulatory bodies etc. 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 empanelment of CAS/SMS vendors. The CAS and SMS vendors not meeting the required standards and protocols shall not be empanelled or shall be de-recognised, as the case may be. 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.

(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.

Comments :-

Such Entity/Autonomous body which is set up giving proper representation to key stakeholders may work on the identification and elimination of loopholes in the existing CAS/ SMS functionalities and to further develop a standardized framework for their operationalization. The same can be done in consultation with all the stakeholders viz the broadcasters, the DPOs, the technology vendors, members of R&D centres, technical experts, regulatory authorities etc.

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.

Comments :-

We suggest that the Autonomous Body or the Entity which is proposed to be set up shall carry the testing and certification of CAS and SMS systems including technical standards for the STB. In view of the specific requirement and ever changing technology, there will be a requirement of re-certification at every gap of time. Hence the re-certification of such systems shall at least be done once in a year.

(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?

Comments :-

The following precautions may be taken:

- The implementation has to be in a phased manner so that abrupt disruptions are not caused
- The same should be backed by regulatory framework and effective implementation provisions through fiscal disincentives etc.
- The cost of such standardization and certifications should not be very high
- The other objectives such as STB interoperability should be given due consideration
- There should be registration of CAS and SMS vendors in India
- Defined timelines for tests and certifications
- Use of advanced embedded systems
- Setting up of an autonomous or independent body

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

Comments :-

The Authorized Officers shall be made more vigilant about the piracy issue. On repeated violations, there should be provisions for suspension/cancellation of DPO license immediately. The Autonomous Body may set up a dedicated team within itself which can look into continued compliance and for effective co-ordination with Authorized Officers in States.

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?

Comments :-

There have to be an effective implementation mechanism backed by provisions for fiscal disincentives / other penalties. The Autonomous Body should be given powers to impose penalties on errant players. Further, on the recommendation of this Body/ TRAI, suitable action may be taken by the Ministry of I&B under the CTN Act and the Uplinking Guidelines. A reference can also be made to the Authorized Officers in Districts to curb the piracy. The compliance of the standards should be made part of the license conditions of the DPOs. A timeframe of about one year may be kept in mind for full implementation of the new framework so that there is enough timeframe for migration to new framework.

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.

Comments :-

The standardization and certification of CAS and SMS will be beneficial to the entire broadcasting system. Though it is likely that the new standardization process may result in some operational issues and additional costs, but there may be foreseeable benefits like:

- A robust system governing the broadcasting ecosystem
- A strong mechanism against piracy, protecting the revenues of broadcasters
- Smooth relationship between service providers as there will be lesser trade disputes
- Will help smaller players to adapt a tested and certified system, thereby giving better access to broadcaster's content
- Non-dependency of DPOs on uncertified Third Party solutions
- Proper accounting and subscription revenues
- Easy and timely audit; elimination of multiple audits resulting in cost savings for all stakeholders
- Greater choice to consumers and uniformity of services
- Proper itemized billing for consumers

- No loss of taxes for the exchequer
- Interoperability of STBs
- Standardized processes across different networks
- Greater and efficient use of EPG by viewers

Q9. Any other issue relevant to the present consultation

Comments :-

At present, the key constituents of DAS system i.e., CAS and SMS vendors are not accountable to any authority. The entire discussion around them happens and stipulations are made without their effective presence. This sometimes results in their non-responsible behaviour which aids unethical practices in the entire system. A provision may be made which makes it compulsory for the CAS and SMS vendors to have an Indian address and there should be a process for their registration with the proposed Autonomous Body so that there is an authorized representative who could be contacted for any clarification/ support for their respective CAS/SMS systems. This will address issues such as delay in providing service support, demand of excessive charges for services, software modification etc. by these vendors and to a large extent will bring in the much desired accountability on the part of CAS/SMS vendors. This will also help in tight integration of the CAS/SMS.

The MSR submitted by DPOs on their letter heads at present should ideally be an auto generated report from CAS/SMS system so that there are lesser possibilities of manipulation / mistake by DPOs and a system should be designed so that the reports can be directly sent to the respective broadcaster through auto generated emails on weekly basis as per the frequency given in the Regulations.

The overt fingerprinting schedule should be made and mandated that it is done on a regular basis to prevent piracy.

We request you to take our above comments on record.

Sanjay Agarwal
Times Network
June 3, ’20.