May 20, 2020

Shri Anil Kumar Bhardwaj
Advisor (B&CS)
Telecom Regulatory Authority of India (TRAI)
Mahanagar Door Sanchar Bhawan,
J.L. Nehru Marg, (Old Minto Road)
New Delhi, 110002, India

Dear Sir,

The MPA appreciates the opportunity to provide a submission in response to the Telecom Regulatory Authority of India ("TRAI") Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting and Cable Services, which was released on April 22, 2020.

The Motion Picture Association ("MPA") is a trade association representing six international producers and distributors of film and television entertainment. The MPA-represented companies are:

Walt Disney Studios Motion Pictures
Netflix Studios, LLC
Paramount Pictures Corporation
Sony Pictures Entertainment Inc.
Universal City Studios, LLC
Warner Bros. Entertainment Inc.

Our member companies produce and distribute a wide range of film and television content in India. In order to support a thriving creative community, it is important that nothing interferes with the ability of content creators, copyright owners, and licensees to create, distribute, protect and secure content (including from unauthorized copying or dissemination, or to prevent circumvention of technological protection measures or digital rights management).

The submission includes MPA Members' comments on the list of features specified in Schedule III of the Telecommunication (Broadcasting and Cable) Services

No. 1 Magazine Road, #04-07 Central Mall, Singapore 059567 . +65 6253-1033 . www.mpa-apac.org

Interconnection (Addressable Systems) Regulations, 2017 and features that the MPA recommends be considered for addition to the list, in relation to CAS and SMS.

We have further provided detailed input to all of the Issues for Consultation. We remain available for further discussion on the matter at your convenience.

Thank you.

Trevor Fernandes
VICE PRESIDENT, GOVERNMENT AFFAIRS, ASIA PACIFIC

O (65) 6253-1033
M (65) 9108 9959
E trevor_fernandes@motionpictures.org

Submission of the Motion Picture Association (MPA)

Telecom Regulatory Authority of India (TRAI) Consultation on Content Security in Conditional Access Systems (CAS) and Subscriber Management Systems (SMS)

Wednesday, May 20, 2020

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?

The following is a list of the features specified in Schedule III, along with MPA's comments about them as well as comments about features that MPA recommends be considered for addition to the list.

A) Conditional Access System (CAS) and Subscriber Management System (SMS):

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.

MPA COMMENT – We agree that the distributor of television channels should be required to verify that the version of CAS it plans to implement has not been successfully hacked. We believe the distributor should also verify that the CAS is up to date and has not been deprecated by the vendor. All these verifications should be performed before implementation, and regularly once deployed.

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

MPA COMMENT – Agreed.

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

MPA COMMENT – Effective methods and processes should be developed and implemented in line with information security best practices to ensure the Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation of those data, logs or reports that require it.

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.

MPA COMMENT – Agreed. Additionally, there should be hardening of SMS and CAS to prevent defeating the interlock mechanism.

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.

MPA COMMENT – As per our comment under item A)4 above, there should be hardening of SMS and CAS to prevent defeating the interlock mechanism.

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.

MPA COMMENT – Distributors of television channels should use lifecycle management processes to ensure continued compliance with the robustness rules and implement security updates of the CAS vendors. Such lifecycle management should include 'end of life' of unsupported or compromised receiving devices such as STBs.

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

MPA COMMENT – In this context we understand this to mean copy protection technologies, including but not limited to copy control information (CCI) or distributor watermarks embedded upstream of the distributor of television channels. The distributor of television channels should not defeat or invalidate any such copy protection technology.

8. The CAS and the SMS should be able to activate or deactivate services or STBs of at least 10% of the subscriber base of the distributor within 24 hours.

MPA COMMENT – Agreed.

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

MPA COMMENT – Agreed. Successful pairing must initiate a secure authenticated channel that carries the Control Words (CW).

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.

MPA COMMENT – Agreed.

11. The SMS should be computerized and capable of recording the vital information and data concerning the subscribers such as:

a. Unique customer identification (ID)
b. Subscription contract number
c. Name of the subscriber
d. Billing address
e. Installation address
f. Landline telephone number
g. Mobile telephone number
h. E-mail address
i. Channels, bouquets and services subscribed
j. Unique STB number
k. Unique VC number.

MPA COMMENT – Agreed.

12. The SMS should be capable of:

a. Viewing and printing of historical data in terms of the activations and the deactivations of STBs.
b. Locating each and every STB and VC installed.
c. Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.

MPA COMMENT – Agreed.

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

i. The total number of registered subscribers.
ii. The total number of active subscribers.
iii. The total number of temporary suspended subscribers.
iv. The total number of deactivated subscribers.
v. List of blacklisted STBs in the system.
vi. Channel and bouquet wise monthly subscription report in the prescribed format.
vii. The names of the channels forming part of each bouquet.
viii. The total number of active subscribers subscribing to a particular channel or bouquet at a given
time.

ix. The name of a-la carte channel and bouquet subscribed by a subscriber.
x. The ageing report for subscription of a particular channel or bouquet.

MPA COMMENT – Agreed. Effective methods and processes should be developed and implemented in line with information security best practices to ensure the Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation of such data, logs or reports.

14. 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.

MPA COMMENT – Agreed – As with item A)13 above, effective methods and processes should be developed and implemented in line with information security best practices to ensure the Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation of such data, logs or reports.

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.

MPA COMMENT – Agreed. In addition, distributors of television channels should have processes to track repeat offences by individual subscribers, such as tracking frequency of an offender being added and removed from the service and other applicable fraud monitoring to drive down fraudulent behavior and piracy.

16. It shall be possible to generate the following reports from the logs of the CAS:
a. STB-VC Pairing / De-Pairing
b. STB Activation / De-activation
c. Channels Assignment to STB
d. Report of the activations or the deactivations of a particular channel for a given period.

MPA COMMENT – Agreed.

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.

MPA COMMENT – No comment.

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.

MPA COMMENT – We agree that a distributor should ensure support for a CAS and SMS system, however we do not agree that such support must be located in-country: a vendor does not have to have a presence in a country to provide support there.

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.

MPA COMMENT – Agreed.

20. Upon deactivation of any subscriber from the SMS, all programme/ services shall be denied to that subscriber.

MPA COMMENT – Agreed. In addition, access to content stored locally by the subscriber should be made unavailable to view e.g. prevent playback of licensed content from Digital Video Recorders.

21. The distributor of television channels shall preserve unedited data of the CAS and the SMS for at least two years.

MPA COMMENT – The term 'data' should be more clearly defined. This item is similar to item A)14 above but brings the SMS into scope. As with item A)14, we recommend that methods/processes be developed in line with information security best practices to ensure the Confidentiality, Integrity, Availability, Authenticity, and Non-Repudiation of such reports.

<u>Additional CAS features recommended by MPA</u>

- Each CAS vendor should define and make available Compliance and Robustness rules (C&R) that are complete.
- An effective documented answer to hack procedure of the CAS vendor should be required.
- The crypto period should be short enough considering the size of the CW.
- The elements of the CAS in the STB should be protected against reverse engineering and tampering, for example:
  - Through the use of a Secure Execution Environment.
  - If it is software-based, through protection of the code and appropriate expertise of the implementers.
  - Through the use of a Secure Video Path.
- The CAS should protect against a list of known attacks, including CW sharing, smart card pairing, Entitlement Management Message (EMM) filtering, hot reboot and standby wakeup, etc.
- Appropriate restrictions on the deactivation of the JTAG (a standard adopted by the Joint Test Action Group) and debug mode.

- A renewal mechanism that is efficient and easy to deploy.
- An anti-rollback mechanism that is implemented appropriately.
- The STB (and smart card if used) should have a revocation mechanism.
- Clarity about who owns the STB's Root of Trust (RoT) and who signs the code of the CAS used by the STB.
- A secure mechanism by which the CAS secret keys are provided in the factory, with safeguards against or about human intervention.
- Addressing the issue of whether the scrambling of audio uses a CW that is different from the one used to scramble video.
- Finally, the issue of on-going fraud monitoring and prevention by the operators should be examined, to clarify whether the existing regulatory requirements include it or, if they don't whether they should.

B) Fingerprinting:

MPA COMMENT – As a general comment, we note that some terms have more than one meaning, depending on the context. In the STB context, fingerprinting means *displaying device-specific information*, e.g., to identify which device or account is redistributing content. The same term is also used in the context of content security on the Internet to refer to the extraction of video fingerprints for use by automatic content recognition systems to *identify copyrighted content, e.g., on upload to a website*. In the general context of video security, watermarking refers to the *insertion of any forensic mark into the content,* including both visible and invisible watermarks.

1. The distributor of television channels shall ensure that it has systems, processes and controls in place to run finger printing at regular intervals.

MPA COMMENT – The need to implement session-based forensic watermarking should be driven by the nature of the content to be carried on the service. As stated in the consultation, carriage of Premium Video on Demand titles should adhere to the Movielabs Enhanced Copy Protection (ECP) requirements and other content protection requirements where such content owner requires it. Further, we note that sports content may require additional protections, and that there may be additional (e.g., contractual) requirements, and/or local legal requirements (imposed, e.g., by copyright and copyright enforcement legislation or regulation) to identify the source of piracy or unlicensed redistribution. These and other factors should be used to determine whether watermarking solutions must or should be implemented within receiving devices.

2. The STB should support both visible and covert types of finger printing.

MPA COMMENT – see comment under item B)1 above.

3. The finger printing should not be removable by pressing any key on the remote of STB.

MPA COMMENT – Watermarks and fingerprints should not be removable on or by any receiving device by any means other than a command from SMS and CAS. In addition, per our comment under item A)7 above, copy protection technologies including but not limited to copy control information (CCI) or distributor watermarks embedded upstream of the distributor of television channels should not be removed or obfuscated by receiving devices.

4. The finger printing should be on the top most layer of the video.

MPA COMMENT – The implementation of watermarking should be such that it is effective whenever video content is presented to viewers via receiving equipment.

5. The finger printing should be such that it can identify the unique STB number or the unique VC number.

MPA COMMENT – Watermarking solutions should be effective in identifying the equipment used, the time, or session. In addition, where applicable, it should be able to identify the subscriber or viewer account, Channel ID, Content ID, unique device identifiers, VC numbers etc. and any other relevant information such as may be required to perform an investigation taking into account applicable privacy laws.

6. The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), Settings, blank screen, and games etc.

MPA COMMENT – Watermarking should be applied whenever licensed content or any part of it is visible on screen whether as Picture in Picture, under a menu overlay such as an EPG of menu, etc.

7. The location, font colour and background colour of fingerprint should be changeable from head end and should be random on the viewing device.

MPA COMMENT – we read this as a reference to visible watermarks: to be effective, visible watermarks should translate across the screen in a random pattern. This is particularly relevant where commercial subscriptions rather than residential subscriptions are used in such places as sports venues, bars, etc.

8. The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the VC.

MPA COMMENT – see our comment under item B)5 above.

9. The finger printing should be possible on global as well as on the individual STB basis.

MPA COMMENT – Agreed, to the extent that distributor watermarks should be capable of being carried through the distribution workflow. Distributors of channels may wish to

implement additional watermarks in relation to managing their device estate, but such marks should not invalidate or obfuscate other watermarks already applied.

10. 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.

MPA COMMENT – we read this as a reference to visible watermarks. Visible watermarks should be displayed without alteration or obfuscation on receiving devices.

11. Scroll messaging should be only available in the lower part of the screen.

MPA COMMENT – No comment.

12. The STB should have a provision that finger printing is never disabled.

MPA COMMENT – Agreed.

13. The watermarking network logo for all pay channels shall be inserted at encoder end only.

MPA COMMENT – we read this as a reference exclusively to a visible watermark or channel logo inserted as part of the video feed prior to distribution to viewers. This may be inserted by the channel playout or by the distributor of television channels as agreed between them.

C) Set Top Box (STB):

1. All STBs should have a Conditional Access System.

MPA COMMENT – For all pay services Conditional Access Systems (CAS) or other equivalent control system such as Digital Right Management (DRM) must be implemented to ensure only authenticated and authorized subscribers can access the system.

2. The STB should be capable of decrypting the Conditional Access messages inserted by the Head-end.

MPA COMMENT – Only for those systems where the user is a subscriber, although we note that some CAS can request the STB of any user to display a message, independently of content descrambling.

3. The STB should be capable of doing finger printing. The STB should support both Entitlement Control Message (ECM) and EMM based fingerprinting.

MPA COMMENT – Agreed: the STB should be capable of applying a visible or forensics watermark triggered by ECM and/or EMM.

4. The STB should be individually addressable from the Head-end.

MPA COMMENT – Agreed.

5. The STB should be able to receive messages from the Head-end.

MPA COMMENT – Agreed.

6. The messaging character length should be minimal 120 characters.

MPA COMMENT – It should be of an appropriate length for an effective system.

7. There should be provision for global messaging, group messaging and the individual STB messaging.

MPA COMMENT – Agreed.

8. The STB should have forced messaging capability including forced finger printing display.

MPA COMMENT – Such functionality could be useful in terms of user communication or forcing of visible watermarks.

9. The STB must be compliant to the applicable Bureau of Indian Standards.

MPA COMMENT – No comment.

10. The STBs should be addressable over the air to facilitate OTA software upgrade.

MPA COMMENT – Agreed, such that the requirements we recommend under item A)1 are met.

11. The STBs with facilities for recording the programs shall have a copy protection system.

MPA COMMENT – Agreed. Specifically, we recommend that such recordings be cryptographically linked to the recording device and that access to such recordings be limited to both the subscriber account that made the recording as well as the device that made the recording.

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?

MPA COMMENT –Not all CAS & SMS vendors comply with all the requirements. Per our comments above, initial audits of the vendors' CAS and SMS systems, and regular audits of their implementation by distributors of television channels would help improve the compliance profile across all technology vendors and implementors. Such audits should be performed by trusted third parties.

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?

MPA COMMENT – Agreed. All "published" standards of content protection have such a framework. At a minimum, they define a C&R regime, which includes a baseline of protections to be implemented and a potential level of robustness. However, the framework could be more detailed than just C&R. For instance, the French government cybersecurity agency (ANSSI) published a draft framework for an evaluation of the security of software of STBs.[1]

We believe that such a framework would result in consistency that would reduce the cost of auditing, improve the robustness of implementation and make the economics of content distribution more favorable to all parties in the content distribution chain and ultimately to the consumers.

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?

MPA COMMENT – No comment.

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.

MPA COMMENT – While MPA does not have a position on what entity should be entrusted with this task in India, MPA and its member studios would appreciate an opportunity to participate in and support such a process, given the experience we have gained in the creation

[1] "METHODOLOGY FOR THE SOFTWARE EVALUATION OF SET-TOP BOX FOR FIRST LEVEL SECURITY CERTIFICATION." ANSSI, Jan. 2015, https://www.ssi.gouv.fr/uploads/2015/01/methodology_for_the_software_evaluation_of_set-top_box_for_first_level_security_certification_en.pdf

of similar compliance models for established standards such as DTCP, HDCP, AACS, AACS2, or ECP.

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.

MPA COMMENT – No comment.

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?

MPA COMMENT – The first model – a designated agency to carry out the testing and certification – is the one used by China DRM. The China DRM laboratories are the exclusive agency to certify China DRM implementations. This model has the advantage of having a consistent quality of evaluation amongst all candidates. Good security evaluation is never purely quantitative. Thus, the submitting manufacturers and CAS designers may appreciate consistency. In the case of a flourishing market, one unique lab can become a bottleneck, so it is important that a lab with sufficient capacity be chosen.

The second model – testing labs accredited by the standards making agency/government to perform testing and certification – is the one used by AACS2. The AACS2 committee defined a list of accredited labs for evaluating the AACS2 implementations. This model is better adapted to a large market, but depends on the experience and expertise of the accredited labs. Therefore, lab selection is extremely important. Currently, several labs in the world have a successful track record of assessing the quality of CAS/DRM implementations, both hardware-based and software-based. Furthermore, as they have evaluated many systems around the world they have accumulated a rich knowledge of the most up-to-date hacking techniques used

by attackers. To mitigate the risk of lack of consistency of evaluation, a rigorous selection and continuous monitoring of the accredited laboratories is essential.

A hybrid model could also be considered. The robustness of the implementation of a CAS is usually a one-time evaluation. Therefore, the evaluation of this robustness occurs before launching the product in the market. The second model may fulfill this type of assessment. However, many security threats can manifest themselves at any point in the lifetime of a product (e.g., a broadcaster may switch off ECM encryption at any time). On-going monitoring is therefore necessary, for which the first model seems best.

Finally, security is a never-ending process as new threats develop, and new vulnerabilities are discovered. Therefore, it is essential to regularly analyze the current landscape and update the C&R. Of course, the new regime is only applicable to newer products with a negotiated sunset period. For instance, the MovieLabs' ECP has undergone several revisions, each of which includes new requirements that mitigate newly discovered attacks.

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.

MPA COMMENT –Per our comments under Q3 above, we believe that standardization *of the framework for certification of the CAS and SMS* (rather than standardization of the actual CAS and SMS) would result in consistency that would reduce the cost of auditing, improve implementation and make the economics of content distribution more favorable to all parties in the content distribution chain and ultimately to the consumers. This should include requirements to audit, as mentioned in our response to Q2 above.

We believe however that the standardization of CAS/SMS (and of DRM) themselves should not be mandatory, but that the security evaluation should be mandatory following some approved framework and C&R. The evaluation may define several levels of security. Distributors would get correspondence between the security level of the CAS and the quality and window of the content they may get. Such an evaluation rating would simplify the discussion between distributors and content providers. Additionally, if the accreditation removes from the market, or at least segregates insufficiently robust CA/DRM systems, piracy would decrease, to the benefit of the entire media ecosystem and of consumers who would receive greater access to copyrighted content.