Questions from the Consultation Paper and answers

Q1 – Features list

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 above mentioned Schedule III holds the following features:

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.

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.

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

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.

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.

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.

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

(B) FINGERPRINTING:

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

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

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

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

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

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.

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

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

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

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.

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

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

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

(C) SET TOP BOX (STB):

1. All STBs should have a Conditional Access System.

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

3. The STB should be capable of doing finger printing. The STB should support both Entitlement Control

Message (ECM) and Entitlement Management Message (EMM) based fingerprinting.

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

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

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

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

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

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

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

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

REMARKS AND SUGGESTED UPDATES TO TRAI'S SCHEDULE III

A1 – Proven history of being hack free.

In many historical hack cases, it was not the CA system that got hacked, but it was the implementation in the client device. CAS vendors therefor need to have an OEM (client device manufacturer) certification program, which certifies manufacturers and does Device Verification Tests of the CAS implementations. Operators and DPOs should insist on successful Device Verification Tests and should get the confirmations of these directly from the CAS manufacturer.

A6 – OTA upgrading capability

Next to facilitating OTA firmware upgrades, the CAS system shall only be able to play out firmware upgrades that have been signed by the CAS vendor. The client devices shall only be able to upgrade to new firmware if the OTA firmware has been signed correctly.

The CAS system shall have a mechanism in place to enforce firmware upgrades on client devices. In this way, if firmware upgrades somehow are blocked at the subscriber end, the client device will lose the possibility to decrypt any channel, until the device has been upgraded to the latest firmware.

The same applies for Viewing Cards in use: it shall be possible to securely renew the software on the Viewing Cards and to block the correct working of Viewing Cards for those to which software upgrades have been blocked

A15 – Blacklisting VCs and STBs

The CAS system shall associate subscribers and their entitlements to specific hardware devices. This way, by de-entitling or de-activating a subscriber, the respective hardware device (VC or STB) can no longer be used and is effectively blacklisted.

.

Q2 – Compliance certificate

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?

It is highly desirable that any new deployment would be based on STBs and CAS with a hardware root of trust enabled, and that systems without would not be allowed anymore for new deployment. In a migration scenario to this, the policy could be set that premium content would only be made available to subscribers with STB/CAS combinations with a hardware root of trust, such that initially content with the most value is protected best.

Q3 – Framework need

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?

Yes there is a need to define a framework for CAS systems to benchmark the minimum requirements

Q4 – Safeguards

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?

Supply contract with CAS and SMS vendors need to include conditions that errors will be fixed according to Warranty and Service Levels. Not fixing errors in time shall lead to penalties and repeated occurrences shall lead to the possibility for the broadcaster to cancel the supply agreements.

Q5 – Framework definition

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.

A committee under BIS with participation from stake holders and experts on the subject like representation from DVB, 3rd party CAS certification companies like Cartesian.

Q6 – Suitable model for compliance mechanism

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.

a) Independent and accredited testing labs shall be entrusted with the certification of the vendors. Companies like Cartesian have proven to be very capable of auditing CAS systems, and might be interested to also run a certification scheme for the TRAI.

b) Introducing standardization and certification into an existing business can be challenging. It will need a long lead time. Easiest and most efficient way of introducing is to make it obligatory only for new to be deployed set top boxes.

Q7 – Mechanism for ensuring compliance

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?

A framework comprising testing and certification, in a running business, can only be set up when this is being introduced gradually, with an announcement/introduction period and a migration period. Our suggestion would be to have an announcement period of 3 years, meaning that from the moment of announcing (all specifications and framework needs to be final by then) and the start date of certifying newly to be introduced set top boxes there will be a period of 3 years. From that date, all newly to be deployed set top boxes need to be certified.

Q8 – Effects of standardization and certification of CAS and SMS

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

Standardization and certification will bring improved quality of service and end-consumer experience. Operators might debate the economic efficiency of it, but by using certified STBs and CAS, the amount of piracy will reduce.

Q9 - Any other issue relevant to the present consultation