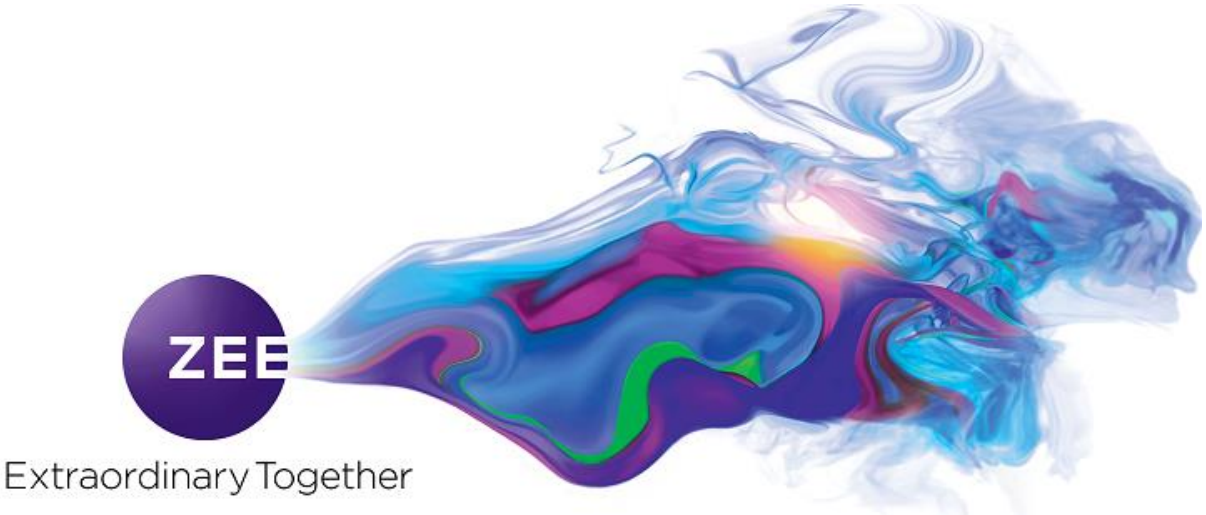
Response of
Zee Entertainment Enterprises Limited

to the
Consultation paper on
Framework for Technical compliance of Conditional Access System (CAS) and Subscriber Management System (SMS) for Broadcasting & Cable services

Issued by TRAI on 22nd April 2020



At the outset we would like to thank the Authority for bringing this consultation paper as broadcasters have been facing several issues regarding correct reporting of subscribers by DPO's. There have been numerous cases faced by broadcasters wherein there was lack of cooperation of CAS/SMS and Headend vendors. We are happy that TRAI recognises the multiple challenges faced by broadcasters in the correct reporting and auditing of CAS and SMS systems. While we appreciate that this consultation paper is trying to bring CAS and SMS Vendors within the ambit of Regulation, we would like to highlight that Multiplexer (MUX) and Headend systems must also be included in this exercise. The reason is that channel name or channel id is just an identifier in SMS and CAS systems and the real conversion of that identifier to the actual channel content is done in the MUX or headend. Unless MUX and headend is included in this exercise there is every likelihood that entire purpose of this exercise would get diluted as there would be a big loophole which could be used for under reporting of channel-wise count.
These comments are based on the questions mentioned in Consultation paper issued by TRAI on 22-04-2020 on Framework for Technical compliance of (CAS) and (SMS) for Broadcasting and Cable Services.

Ques No. 1: List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?

Response: Important features of CAS in addition to Schedule III requirements

1. CAS should have multilayer CAS system installed on chip (SOC) so that in case first CAS gets compromised then second CAS installed on chip can be enabled on the same STB without delay.
2. Scrambling should support 128 or higher bits key for better encryption system.
3. ECM, EMM and control words to be encrypted with strong encryption. The CAS system must have a hardware-based security core which is tamperproof in every STB.
4. EMM key should be highly secure and it should not be possible to extract EMM/control word out from STB. Hacking involves the access to the "Control Word' and its propagation over the internet so that it can be inserted separately without the VC. The only way to prevent this 'is to have card less CAS set-top boxes, equipped with a hardware-based root-of-trust. A hardware root-of-trust, provided by platforms such as Crypto Media, offers operators robust security protection with an integrated security core (SOC) which cannot be tampered with and the "Control Word" is not under communication outside the security core protected SOC. The Advanced embedded type CAS would require the CAS specific secret keys to be fused in the SOC thus making it secure against hacking.

5. STB should have chipset level pairing.

6. All current and historical data/configurations (SID, Product detail, Historical package channel composition, Product logs, AC data, ECM, EMM data) of CAS server including back up/child servers to be recorded in database with time stamp and system should not have provision to delete/modify any logs. For the sake of analogy, it should be like a flight recorder/blackbox of an aircraft from which nothing can be deleted, once a log is written nothing could be deleted from this log even by the CAS Vendor itself.
   This has been observed during Audits by TRAI empanelled Auditors that both subscriber data and logs of CAS and SMS systems are replaced by manipulated logs. Thus, making auditing an ineffective exercise.

7. System should be able to detect and disable control word sharing & compromised EMM/ECM key. *Hackers are able to separate control word from the feed and they sell the keywords through internet thereby causing loss to Government, DPO and Broadcasters.*

8. CAS System should be able to detect and disable cloning of STB. There should not be more than 1 STB number with same UA and/or serial number. Each STB should be individually addressable. There are reported cases of cloning of STBs, whereby hacking of secure key of a STB, it was cloned into several STBs while only the One hacked STB reflected in the system. This is another instance of piracy resulting in leakage of revenue.

9. CAS server (all ECM/EMM/any servers installed in field) should capture all commands and user level logs with date and time stamp. The logs should contain complete commands including time stamps and type of command and channel/product/package activated or deactivated. The logs should be in such a format and should contain enough information that Auditor working on the logs should be able to derive all relevant information including channel-wise count of historical period accurately. *While conducting audits TRAI empanelled auditors have observed that in a lot of CAS/SMS systems the logs do not contain adequate information and are incomplete which makes the logs of no use in determining accuracy of reports. In some of leading CAS systems also the logs are generated in such a format that they are either not readable, or they are unstructured which restricts analysis on a set of logs for comparison with CAS data.*

10. All data including logs to be available in tamper proof in live server(s) for at least two years. In case DPO's have issue in saving non editable logs in live server due to server capacity/data size issues then TRAI should have a mechanism where logs are written to a central server residing with TRAI/Certification(trust) Authority on real-time basis.

11. Complete data and all logs to be backed up in secure manner. All logs (transaction, user and command level) to be tamper proof and any change (edit/deletion/enable/disable) in configuration of any data including SID, AC data encryption keys, product/service/package to be captured in logs.

12. While a customer should be activated for a long term so that it remains active with a pack/bouquet/a-la-carte for practically perpetual duration and till such time he is

disconnected by the DPO, however the life of EMM keys should not be more than 1 month at any point in time because in many local/Chinese CAS system it has been observed DPO gave EMM entitlements with expiry period more than 5-10 years. In such scenario DPO can activate some of boxes directly from SMS with EMM entitlement for 10 years and after that Delete some of the records from the database and logs or send deactivation from SMS but disconnect CAS link or remove boxes from signals so that box should not receive DA request and after expiry of DA period boxes put on signals and it will continue active for next 2 years but these boxes will not appear or appear in DA status in SMS & CAS. For Example in a widely used CAS system which VC number and the Product id (channel enabler) is activated for a longer period (say year 2039) however the EMM is activated for 60 days only at any point in time and the date is extended by 15 days after every 15 days in multiple batches.

Since Cable and DTH is one- way technology wherein STB channel entitlements are sent from CAS and they reside on the STB itself and STB does not check back with CAS for channel authorisation. Some DPO's have been misusing this by sending activation and enablement commands for a longer period and then deleting the records and logs from the system. This has been observed in a lot of Audits that services activated on STB's are different from the information stored in CAS/SMS.

13. It should be mandatory to send periodic (period should not be greater than 20 days) fresh EMM keys so as to ensure that all old EMM keys get updated at STB end. The STB software should be secured in such a way that no EMM is ever blocked/rejected by STB. *This has been observed that a STB is hacked and DPO is not able to send any deactivation or fingerprint command to control the STB. Such STB's then is used by hacker for providing signals on illegal OTT apps and source of signals can neither be identified nor stopped.*

14. The EMM addressability in individuals/groups/ region/global/LCO should be possible. There should be capability so that EMM keys can be sent on geographic locations based on pin code, city, etc. The STB should work in that particular area or pin-code and should not work in any other area or pin-code.

15. CAS servers should be robust and have cyber and data security to avoid probability of any backdoors and malicious software attacks. The Security software should be upgradeable, and upgrades should be provided by vendor during the entire lifetime of CAS). *A lot of DPO's including some Big DPO's have informed Broadcasters and Auditors that their CAS and SMS systems have been attacked by virus or cyberattack has happened, and hacker has encrypted all the data.*

16. CAS system should have strong blacklist command that can kill Chip data of STB or kill View card so that same card/STB cannot be re-deployed by the DPO.

17. In case of any hacking or compromise of CAS server, CAS system should be able to deploy patch within two weeks to disable such hacking.

18. Fingerprinting/watermarking mechanisms should provide a mechanism to block access of content to compromised devices/ network in case of a security breach. It has observed that substandard CAS systems do not have strong fingerprinting and they do not also have secure EMM mechanisms, hence they are not able to block access of content to compromised STBs.

19. Finger printing should be on top layer of video so that no malicious software is able to disable or mask finger printing. The STB software should have provision to flash FP on topmost video layer.

20. CAS system should have strong and secure boot loader in STB to ensure no malicious software can compromise STB.

21. CAS system should have strong security feature implemented to ensure that STBs of one network should not operate in another networks. The AC data of each channel should be unique for each network. It has been observed that some of Chinese CAS have configured common AC data for all networks and STB works in any of these networks. In such case in one network, these STBs will show in DA status, but same STB works on another network with same CAS system. *This has been observed in some DPO's (say DPO A) that activated STB's of a particular CAS if installed to any other DPO (say DPO B) using same CAS then the STB works perfectly. When audit of DPO A is conducted he does not own of such STB's and neither does DPO B owns up such STBs. The problem is much more complicated in reality as there are more than 50 DPO's where these STB's are interchangeable.*

22. CAS system should be able to detect if there is any common ECM PID mapped to multiple channels/AC data in MUX. *DPO's and CAS vendors use same ECM for multiple channels, if 1 channel is activated from SMS and CAS then all channels get enabled on the STB which share the same ECM PID. This has been observed in a lot of DPO's in NTO.*

23. Each CAS vendor should declare the database tables which is used to store VC level, Entitlement Level information and database structure of reporting module. There should not be any active unique subscriber residing outside these tables. Any change in structure of these tables should be approved by agency certifying the CAS. There should not be an option to split CAS database or for creation of more than 1 instance by DPO or vendor. Database of CAS should be secure enough to ensure that no one can manipulate the same. *CAS Vendors do not maintain uniform table structure for subscriber data and the table structure is customised for each DPO, this is sometimes done to under report subscriber base wherein subscribers and logs for a set of subscribers is hidden and not declared. In absence of declared table structure Auditor has to rely on whatever data is provided by the DPO/ CAS vendor which results in ineffective audit as subscriber base is systematically hidden by DPO, SMS & CAS Vendor.*

24. CAS Vendor should maintain a detail of CAS servers authorised by him for each DPO and such data should be provided to TRAI empanelled Auditors when they seek this data. In case any DPO has installed backup, server and connected to main server, CAS system

should have some intelligence to track the instances where backup server has been used as main server. All logs of backup server to be maintained by main server also. The CAS should have a mechanism to check and ensure that Main and Backup servers have exactly same VC and Entitlement level information and the servers are synchronised. *CAS Vendors do not maintain information on number of servers allocated/installed for a DPO and related entities, this is sometimes done to under report subscriber base wherein subscribers and logs for a set of subscribers is maintained in a separate server which is hidden and not declared. The hidden/undeclared servers are sometimes purchased and installed by entities which are sister entities of the DPO, but such CAS is integrated with additional MUX installed in remote/mini digital headend. Since the CAS is of same vendor, the same is not easily identifiable as separate CAS in TS recording .In absence of declared table structure Auditor has to rely on whatever data is provided by the DPO/ CAS vendor which results in ineffective audit as subscriber base is systematically hidden by DPO, SMS & CAS Vendor.*

25. The SMS and CAS should always be in absolute synchronization. However, issues are raised from time to time from field in this regard. CAS system should be able to identify if CAS integration happens with more than one SMS system (whether its mirror or child SMS system).

26. SMS & CAS system should be real time integrated and auto reconciliation of VC and service level between SMS & CAS database to be implemented and all variance reports should be available in system with time stamp.

27. CAS database should have all reports of whitelist of card/STBs with date and time stamp. CAS vendor should release XML/secure un-editable file of keys/card detail purchased by network and upload in CAS server directly and the same should capture in logs also. *In a lot of cases, DPO does manipulation in the database for reporting and auditing and provide filtered data, however if CAS vendor maintains whitelist of all VC's allocated to a DPO then the risk of hiding subscriber base is reduced.*

28. There should be provision of TRAI empanelled Auditor to Audit CAS vendor (Apart from DPO Audits already in place) on any deployed system within India and CAS Vendor to be held accountable if any deliberate misuse/under reporting is found in the system. *In the Audits of DPO system, DPO's attribute a lot of discrepancy to the CAS vendor or CAS product. There is requirement of Audit of CAS vendor himself on installed systems so that the responsibility of under reporting can be fixed and under- reporting is stopped.*
29. In addition to CAS and SMS systems other related addressable systems like MUX, DHE & STB plays important role in terms to content security and factual reporting of subscriptions. We suggest including MUX also in addition to SMS and CAS system to have minimum security requirement to ensure content security and actual reporting of subscription.

Important features of SMS in addition to Schedule III requirements.

1. SMS & CAS system should be real time integrated and auto reconciliation of VC and service/channel information between SMS & CAS database to be implemented. variance report should be available in system with time stamp and should be captured in logs also. As such, the SMS and CAS should always be in absolute synchronization.
2. It has been found in few cases that there may be mirror SMS which are able to configure subscribers, does not reflect subscribers' information in main subscriber database. This issue has multiple implications. Firstly, it results in improper reporting of subscription figures. As revenue sharing under the regulatory framework is subscription based, this has serious financial implications. On the other hand, synchronization issue also has implications on service provisioning to consumer. For example, this may result in a situation where a program/channel has been subscribed to a particular customer/STB but due to integration problem it may not reflect in CAS and the consumer may remain deprived of the service. SMS should be able to identify if any mirror SMS or child SMS created by DPO.
3. Complete data to be backed up in secure manner.
4. All logs i.e. user, command and configuration level should be in readable, understandable and analysable format. *While conducting audits TRAI empanelled auditors have observed that in a lot of SMS systems the logs do not contain inadequate information and are incomplete which makes the logs of no use in determining accuracy of reports. In some of SMS systems the logs are generated in such a format that they are unstructured which restricts analysis on a set of logs for comparison with CAS data.*
5. All logs to be stamped with date and time and system should not allow any alteration or modification of any logs. For the sake of analogy, it should be like a flight recorder/Blackbox of an Aircraft from which nothing can be deleted, once a log is written nothing should be deleted from this log even by the SMS Vendor itself. *This has been observed during Audits by TRAI empanelled Auditors that both subscriber data and logs of CAS and SMS systems are replaced by manipulated logs. This makes auditing an ineffective exercise.*
6. SMS servers should be robust and have cyber and data security to avoid probability of any backdoors and malicious software attacks. *A lot of DPO's including some Big DPO's have informed Broadcasters and Auditors that their CAS and SMS systems have been attacked by virus or cyberattack has happened and hacker has encrypted all the data, or the system crashed and data deleted during such attacks.*
7. In case of any virus attack, system should be able to restore all data and database completely.

8. SMS system should be able to extract all reports from front and back end and all reports should have date and time stamp. *This has been observed during various audits that module created for extraction for Audit data is mapped to a dummy database which has manipulated/filtered data. Extraction of data from backend tables with clear table structure information will prevent such under reporting.*

9. All channels and package configuration detail should be in sync with CAS configuration and any mismatch should be detected by system. The system should do auto reconciliation of channels/ala-carte and all packages with their respective id's created in SMS with CAS configuration and variance report should be available in system with logs. *Auditors have observed in a lot of DPO's that package configuration of CAS has higher number of channels while SMS has lower number of channels which leads to incorrect reporting.*

10. All alter/modification in any configuration of channel/package/report format should be captured in logs. *Auditors have observed in a lot of DPO's that package configuration is changed before Audit wherein some channels are removed. If logs of all such changes is not captured, then Audit becomes ineffective and any information prior to the day of audit cannot be relied upon.*

11. SMS system should show logic/query created for each report and there should be capability to extract reports from front and back end of system.

12. Each SMS vendor should declare the database tables used to store VC level, service Level information and database structure of reporting module. There should not be any active unique subscriber outside these tables. Any change in structure of these tables should be approved by agency certifying the SMS. There should not be an option to split SMS database or for creation of more than 1 instance by DPO or vendor. Database should be secure enough to ensure that no one can manipulate the same. *SMS Vendors do not maintain uniform table structure for subscriber data and the table structure is customised for each DPO, this is sometimes done to under report subscriber base wherein subscribers and logs for a set of subscribers is hidden and not declared. In absence of declared table structure Auditor has to rely on whatever data is provided by the DPO/ SMS vendor which results in ineffective audit as subscriber base is systematically hidden by DPO, SMS & CAS Vendor.*

13. SMS system should not allow to split database or create multiple instances of database.

14. SMS system should capture all activations including testing, demo, VIP package/STBs.

15. SMS should be able to extract report on daily, weekly and monthly basis.

16. SMS should have complete inventory report with following detail
    a. Whitelist detail
    b. Faulty STB/VC – repairable and beyond repairable
    c. Warehouse fresh stock
    d. In stock at LCO end

e. Blacklist
f. Deployed with activation status
g. Testing/demo location

17. The framework should prevent deployment of sub-standard systems in the network.

18. SMS Vendor should maintain a detail of SMS servers authorised by him for each DPO and such data should be provided to TRAI empanelled Auditors whenever they seek this data. In case any DPO has installed backup server and connected to main server, SMS system should have some intelligence to track the instances where backup server has been used as main server. *SMS Vendors do not maintain information on number of servers allocated/installed for a DPO and related entities, this is sometimes done to under report subscriber base wherein subscribers and logs for a set of subscribers is maintained in a separate server which is hidden and not declared. The hidden/undeclared servers are sometimes purchased and installed by entities which are sister entities of the DPO, but such SMS is integrated with hidden CAS at downstream at 2nd or 3rd MUX. In absence of declared table structure Auditor has to rely on whatever data is provided by the DPO/ SMS vendor which results in ineffective audit as subscriber base is systematically hidden by DPO, SMS & CAS Vendor.*

19. There should be provision of TRAI empanelled Auditor to audit SMS vendor (Apart from DPO Audits already in place) on any deployed system within India and SMS Vendor to be held accountable if any deliberate misuse/under reporting is found in the system. *In the Audits of DPO system, DPO's attribute a lot of discrepancy to the SMS vendor or SMS product. There is requirement of audit of SMS vendor himself on installed systems so that the responsibility of under reporting can be fixed and under- reporting is stopped.*

Ques No. 2: As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?

Response: SMS and CAS certificates as per schedule III do not suffice to confirm the compliance in the spirit for which such certification was envisaged in the first place. The purpose of certification from the vendors was meant to be a check on Auditee (which in this case is DPO) by an independent 3rd party which is in control of product and its features. During Audit Manual creation process it was felt by stakeholders that to optimise time of audit completion, the Auditor should rely on the certification of CAS and SMS vendors as the vendors would have structured products with very limited option with DPO to do any major changes in the systems. However, during the Audit exercises, it has been noted by various stakeholders that not only are the installations customised for each DPO as per his requirements by the vendors but there are some vendors/3rd party players who change

configurations/ databases of these systems with the sole objective of under reporting and for enabling piracy. SMS and CAS vendor was actually envisaged to be play the role of Trusted Authority for his product. If vendor certified for the installation at DPO premises, it should have ideally meant a tamperproof system with correct reporting and compliance to schedule III. However, for reasons already given above it is unfortunately not the case for most of the vendors whose products are installed in India. Another issue is that of Inhouse developed systems where DPO himself becomes so called "Trusted Authority/Certification Authority". These inhouse developed systems are developed by same of different legal entity controlled by the DPO and in such cases certification by the vendor becomes mockery of the Audit process and works as self-defeating control mechanism in both pre-signal and post-signal Audits. There is requirement of Trusted Authority/Certification Authority which issues such certificates for each DPO and not only for a product being deployed by a Vendor across various DPO's. Apart from the issues mentioned above there are some more issues with the current systems of issuing certificate by CAS and SMS vendors

a. In most of cases it has been observed that DPO has edited the certificate/s or fake certificate have been provided to Broadcasters. The certificate shared/ provided are old or without any date of issuance. The certificate provided are in form of photocopies and lack any authenticity in absence of digital signatures.

b. The certificate does not include logs and their formats. Certificates are silent on the declaration that all data are intact, and no modification or deletion of data and logs happened. Also, certificate do not provide information about total number of keys/UA/VC data ported in system on the date of issue of certificate.

c. Certificate/s do not provide any understanding on logic on queries used to extract different reports and do not mention even the basic tables that have certified data.

d. In case of any changes in system including database or version change than fresh certificate/s are not provided.

Additional checks required for compliance:

1. Vendor should provide details of database tables and system architecture so that Auditor can validate the subscriber base.
2. The logs should be in readable and analysable formats and should capture complete information and correct date time stamps.
3. Vendor should provide details of all the servers enabled for a DPO and related parties of DPO so that proper audit can be conducted.
4. DPO should provide information of servers enabled for all entities who have taken the system which are related parties of DPO's so that there are no dummy entities running parallel systems to enable under reporting.
5. Most of DPOs are coming up with Hybrid STBs and distributing signals on OTT or IPTV platform so DRM specifications should be incorporated in the certificate and documents.

6. All CAS and SMS systems should be validated for compliance on regular interval by certified authority and in case broadcaster or auditor report any hacking/ piracy due to compromised system then authority should take strong action. In case of allegation is proved then the authority should blacklist vendor for at least 2 years for any new installation/sale.
7. In addition to SMS & CAS, the other related addressable systems like MUX, DHE & STB are vital components in any digital headend and play a major role to ensure content security and correct subscription reporting. Therefore MUX, DHE and STB should also include compliance measures and certification from vendors to be made mandatory.
8. In a huge number of instances, entire system of CAS, SMS is bypassed through the mechanism of local Insertion of channels by LCO. DPO configures some channels in TS but does not insert and Audio/Video, the content of which is actually inserted by LCO downstream. In many instances the content such inserted by LCO is Pay Tv content. While the CAS and SMS would have captured such entitlement as local channel or not captured at all as channel is provided in unencrypted manner. In reality the subscribers are enabled with Pay Tv content. Authority should specifically disallow this in the framework so that no local insertion of content by LCO is possible. All content must be inserted by DPO and must be in his control. Even if local content is to be retransmitted, the same should be done by DPO in his main Digital headend in encrypted mode and should not be left to be inserted by LCO in uncontrolled and unencrypted manner. This current practice of channels which are unencrypted open for local insertion by LCO must be stopped as this is major source of under-reporting and piracy.

Following are the suggested basic requirements of MUX:

a) Configuration of channel and transport stream should be as per DVB standard only.
b) Unique ECM PID for each channel and system should not allow allocation of same ECM to more than one channel/service.
c) Unique access criteria for each channel. System should not allow allocation of same access criteria to more than one channel/service.
d) MUX should have its own database and all logs of all configurations including scrambling, user level and command level to be captured with date and time stamp in the logs. Today a major mode of under reporting is by changing the mapping of AC data in MUX which defeats the purpose of provisioning channels through SMS and CAS.
e) Unique LCN should be configured for each channel and same LCN should not be configured to more than one channel.
f) MUX should pass following data in all Transport streams:
    a. Service provider detail
    b. LCN detail
    c. NIT
g) It should not be allowed to configure any channel or transport stream without content in MUX.

h) MUX should able to detect and disable transmission of any channel without scrambling and encryption from CAS.
i) All Channels should be encrypted in MUX and there should not be any channel without content.

Ques No. 3: Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?

Response:

3.1 There is a need to define the Minimum Basic Functionality (MBF) for every CAS/SMS system to be approved in the country. Irrespective of the technology deployed, the following basic criteria should be met:

a) Hardware based Root of Trust: For all cases where a Card-less CAS is deployed, the CAS system must have a hardware-based security core which is tamperproof in every STB.
b) Support of features of Key Ladder as per standards.
c) Continuous upload of encrypted SMS command data into a cloud base storage, managed by an entity managing an "Account in Trust" or Escrow, which can only be accessed by an Auditing authority but not altered.
d) Multiple algorithm fuse map to change algorithms on the fly at the time of seeking approval.

3.2 Before deployment of any CAS system by any operator, the following procedure should be adapted:

a) The Operator should file a Request for Approval (RoA) giving the CAS version and all relevant details in the proforma provided by the Government Agency responsible for granting approvals.
b) The Proforma should have a section where the CAS vendor also participates and provides details of the CAS system which should inter-alia include the following:
    1) CAS Technology deployed (such as RSA) and hardware-based root of Trust.
    2) Previous hacking history of the CAS system including previous versions.
    3) Provisions in the CAS system to upgrade to a new CAS algorithm using a hardware-based fuse map.
    4) History of CAS deployment.
    5) History of CAS data sharing: Including to STB vendors, SMS vendors and others.
    6) Need for Upgradation of Software version of the CAS in the current financial year, if any.
    7) Time taken for such upgradation and system security during such planned upgradation.

Authority should define strong framework for CAS, SMS, MUX, STB and DHE to benchmark the minimum requirements of the system to ensure better security of content, quality of content, piracy control, cyber security to control hacking/virus attack and data manipulation. All systems installed in DHE specially CAS, SMS, MUX & STB to be certified by authority before deployment or before commencing business in India. The certification process should be transparent and compliance check on regular interval to be implemented.
It is recommended that a Trusted Authority/Certification Authority be nominated which certifies deployment at each DPO, such TA/CA should be of international repute & technically sound body which has reputation and integrity beyond doubt

Ques No. 4: What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?

Response: Whenever any advancement on the technology an upgradation invariably should happen. It is submitted that with every new method invented for piracy, an upgrade of the CAS and/or SMS system and/or STB becomes necessary for fixing the origin of piracy.
In the absence of regular updates and upgrades by CAS and SMS vendors, the security of CAS, SMS and STBs will be compromised making the system more vulnerable and prone to piracy of broadcasters' channels resulting in revenue loss for DPOs, broadcasters and the government. This is in keeping with the fact that any unsupported CAS and SMS will be unable to meet the quality of standards as mandated by the regulation.
The safeguards which are necessary to ensure that the consumers and all other stakeholders do not suffer for want of regular upgrade/configuration by CAS and SMS vendors are as follows –

1. Standard/world renowned CAS and SMS should be installed at DPO premises with standard server and software configurations.
2. The Agreements of DPO and SMS/CAS Vendors should be in written with defined responsibilities and payment schedules. *we have observed during various audits that due to non-payments the CAS/SMS vendors deliberately install various updates to either restrict the services or privileges of the DPO.*
3. Multiple Mergers and Acquisition of DPO's also causes updates in CAS, STB and SMS which causes inconvenience to stakeholders.
4. It has been observed that there are shadow systems deployed at DPO premises, these are the systems for which subscribers are not reported to the government and the broadcasters. Since all these customers are managed discreetly, this leads to unnecessary multiple upgrades to the system to maintain secrecy. For these systems there are no written Agreements and SLA's, due to which subscribers availing services have to face issues.

Ques No. 5: 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.

Response:

a. There are different roles which need to be performed by different set of entities so that checks and balances are maintained and there is concept of Maker, Checker, Reviewer, Auditor and Adjudicator.

b. The role of setting standards for CAS, SMS, MUX and DHE should ideally reside with a multi -disciplinary body which has representation from relevant ministries of the Government, TRAI, CDAC, STQC, Broadcasters, major distribution platforms, major CAS, SMS, MUX, STB, DHE vendors, chip manufacturers, device manufacturers and noted academicians of international repute and TRAI empanelled Auditors. Such an agency could work under direct supervision of TRAI as they are well versed with the intricate issues of the industry and can bring realistic elements in timebound manner.

c. The body/agency drafting standards should not overlap with either the body/agency providing the certification and/or the Body/Agency in the role of Audit of these systems at a later stage. All these 3 units should be watertight and completely mutually exclusive.

Ques No. 6: Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.

a) Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of testing and certification be entrusted with accredited testing labs empanelled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.

(b) What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation?

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

Response: Post development of technical framework for systems including CAS, SMS, MUX, DHE and STB -

a) There should be a designated agency to carry out the testing and certification to ensure compliance to such framework. TEC is the agency which is appropriately placed to carry such testing as they have been doing same for Telco equipment and have processes and procedures in place for same. Independence, reputation and knowledge of a body like TEC

is best for the task. Since TEC has no direct involvement with the routine activities of Broadcasting sector, it will be able to act as an independent accreditor.

b) Considering the rapid evolving of technology, technical framework should be reviewed periodically to ensure that systems are capable to adopt latest technology and are future ready for at least 5 years.

c) To ensure continued compliance need to have following check list for any certification body.

i. Half yearly certificate to be issued to any system.

ii. Independent body to be appointed for validation and compliance check (in field) and submit report quarterly.

iii. In case of any new version release by CAS, SMS, MUX systems then old certificate should become invalid and new certification of software version to be obtained from certification body.

iv. In case any CAS, SMS, MUX, DHE,& STB system gets compromised or hacked or vendor involvement is found in manipulating subscriber reports than that particular vendor should be blacklisted for at least 2 years and all systems deployed in field should be rectified before removal of blacklisting of the vendor apart from a financially penalising the vendor. Such a blacklisted vendor shall support the existing DPO's but shall not be allowed installation of product in a new DPO until he is removed from Blacklist. TRAI empanelled auditors shall verify the vendor blacklisting at the time of causing audit under regulation 10(7) of interconnect regulations 2017.

v. Provision of Audit of CAS, SMS, MUX systems by Auditor of repute on Annual basis where Auditor would validate product of a vendor installed at DPO premises.

Ques No. 7: Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes, please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?

Response: In present scenario where a lot of DPOs have deployed substandard systems especially SMS & CAS systems, it should be mandatory for all deployed CAS/SMS/MUX/STB systems to confirm to the framework. There is a need to take in consideration of all such systems which has history of hacking/data manipulation or cyberattack should not get relaxation; such systems should comply to new framework immediately.

All systems should compliant with all Minimum Basic functionalities (MBF) defined as per framework in phased manner:

Subscriber base	Timelines of Compliance
Less than 5000 Subscribers or More than 1 Lakh subscribers	3-4 Months
5000-1 Lakh subscribers	6 Months - 1 Year

Ques No. 8: Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end- consumer experience? Kindly provide detailed comments.

Response: Yes, implementation of new framework to standardization and certification of CAS, SMS & MUX and STB will bring economic efficiency & improve QOS –

a) Updated secure systems will enable smooth business with less technical issues to DPO which in turn shall lead to better revenue collection from field.

b) Secure and transparent systems shall improve trust in the ecosystem and build business relations in between Broadcaster and DPOs.

c) Secure systems will not allow manipulation data/ logs and shall lead to correct subscription reporting to Broadcasters.

d) True and correct subscription reporting shall lead to enhanced tax collection by Govt. bodies.

e) End consumer will get better experience and quality of service (QOS).

f) Transparency in complete business cycle shall lead to more foreign investment in Broadcasting and Cable business.

Ques No. 9: Any other issue relevant to the present consultation.

Response: TRAI would consider extending the scope of present consultation to MUX, Digital Headend & STB also. The role of SMS, CAS, MUX and Digital Headend are vital in determining correct Channel wise subscriber count. While TRAI recognises the role of CAS & SMS, the role of other related systems like MUX, DHE and STB are equally important.

MUX plays important role in any digital headend. The reason is that channel name or channel id is just an identifier in SMS and CAS systems and the real conversion of that identifier to the actual channel content is done in the MUX or headend.

1. Common ECM PID is configured to multiple channels and in such case one channel activation command is sent from SMS/CAS but all channels with common ECM PID shall get enabled at STB end.

2. Channel and Service ID are configured in CAS, but actual audio/video content is inserted in MUX and linked to channel/Service ID. For Example: FTA channel – DD 1 configured in SMS and in CAS SID -1 and is linked to DD-1 but in MUX some pay channel

like Zee TV content (audio/Video) is linked to DD-1 SID. In such case, DD-1 will reflect in SMS/CAS database and subscriber reports but at STB end, pay channel content shall playout instead of DD-1.

3. DPO configures all Transport streams in MUX but for some channels he does not insert any Audio/Video as a result of which LCO is able to insert a channel at its end. This is specifically done to enable LCO to insert any audio/video /channel in a specified TS. All STBs connected to that particular LCO shall get that content which has been inserted locally but the same shall not reflect in SMS/CAS reports.
4. Same channel audio/video (content) with different EPG name is configured in MUX. For example: Zee TV configured with EPG name Zee TV, SID -1000 & LCN No.1 and another same Zee TV Content (audio/video) configured with EPG name Zeee TV, SID 1001 & LCN No. 900. In such case Zee TV configured with SID 1001 on LCN 900 shall not reflect in SMS & CAS logs and reports.

In order to control piracy and under reporting of subscriber report request TRAI to define Minimum Basic functionality (As mentioned in response to the Question 2.) of MUX in consultation paper.

Glossary	
AC data	Access Criteria Data
CA	Certification Authority
CAS	Conditional Access System
DHE	Digital Headend
DRM	Digital Rights Management
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Programme Guide
LCN	Logical Channel Number
MUX	Multiplexer
NIT	Network Information Table
PID	Packet Identifier
QOS	Quality of Service
SID	Service ID
SMS	Subscriber Management System
SOC	Silicon on Chip
TA	Trusted Authority
TS	Transport Stream
UA	Unique Access (key)
VC	Viewing Card