Introduction

Synamedia welcomes this opportunity to respond to TRAI's Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services, dated 22 April 2020.

Synamedia has been in the pay-TV technology sector for over 30 years including its well known predecessors NDS and Cisco.

The world’s largest direct-to-home satellite, cable and over-the-top video operators, content owners, and broadcasters trust Synamedia to help them generate new revenue streams, embrace internet protocol delivery, and protect revenues.

Over 200 pay-TV operators and half of the world’s top tier pay-TV operators currently use Synamedia products, services and technologies.

Synamedia employs around 3,000 staff globally, around 1,000 of whom are employed in India.

Over two thirds of Synamedia staff are dedicated to research and development, with the Synamedia intellectual property portfolio currently exceeding 900 US and worldwide patents.

Synamedia’s customers in India include DTH operators Airtel and Tata Sky and cable multi-system operators DEN Networks and Hathway.

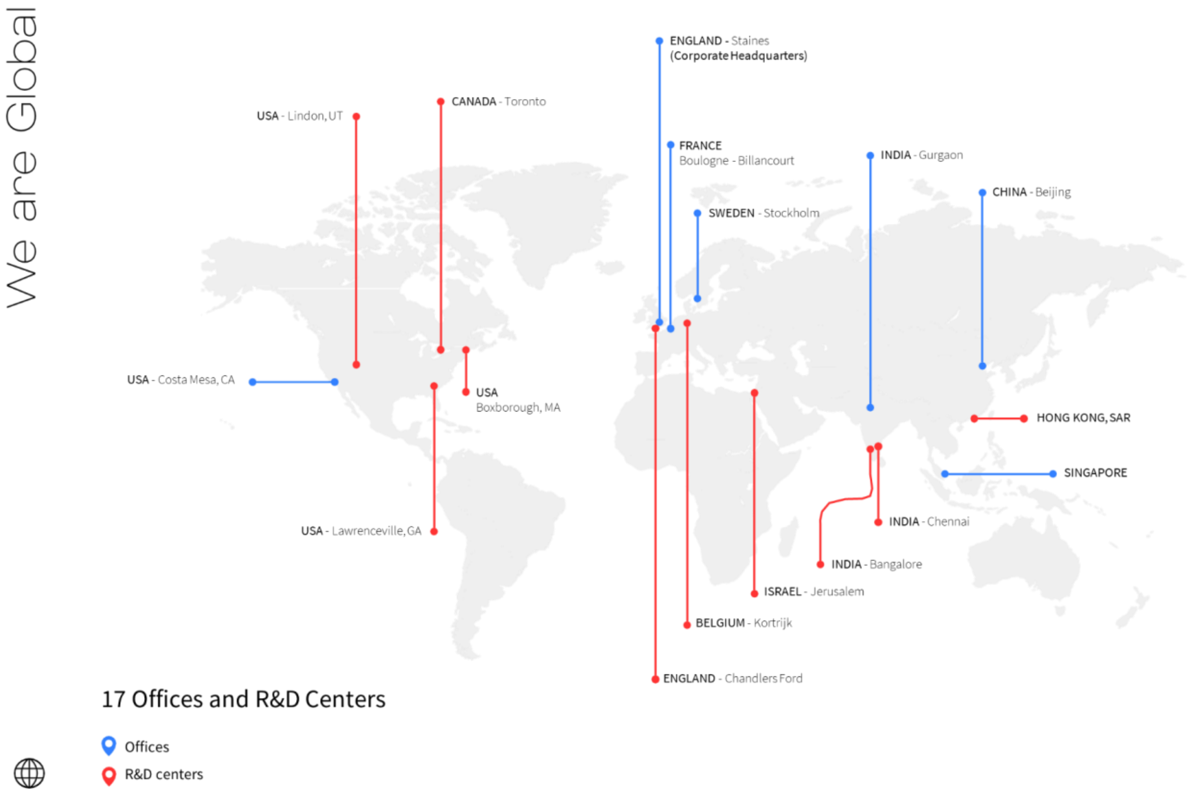

Figure 1 Synamedia Offices and Research and Development Centres Worldwide

Executive Summary

Synamedia limits the scope of this response to the products, services and technologies it offers. Specifically, this **excludes SMS**, but **includes** CAS, set-top-box boot loaders, middleware, applications and software integration, digital video recorder software and integration, conditional access modules including USB key and integration – plus many others not so directly related to this consultation paper.

TRAI prepared and released Schedule III after much industry consultation and deliberation. Meanwhile, India has completed digitalization of the pay-TV sector and operators have deployed more than 160 million set top boxes in the country, with all major pay-TV operators – cable and DTH – having selected and deployed CAS solutions.

As technology innovations continue, state-of-the-art in CAS technology has seen many new upgrades with many new features and functionalities being implemented globally, as well as security enhancements.

Synamedia understands that many operators have deployed inferior sub-standard quality CAS solutions. As a result, they are not capable of implementing or adequately adhering to the new regulations released by TRAI – including the New Tariff Order – and are unable to prevent the piracy of broadcasters's content, which is directly impacting the broadcasters revenue and tax revenues.

As most operators have selected their CAS technology partners, Synamedia recommends that TRAI keep the Schedule III Framework, but **adapt** it with the latest updates to the features already mentioned in Schedule III and **augment** it by adopting recent global CAS innovations to better protect against content and service piracy.

Synamedia recommends TRAI, continue with the Schedule III Framework, but with frequent regular CAS reviews and adoptions of new global CAS technologies and feature innovations. This is more efficient and less disruptive than defining new frameworks every time.

The near-global response to Covid-19 has highlighted one long-known, but until March 2020 less frequently acknowledged major advantage of traditional, dedicated-platform pay-TV services delivered over cable and satellite as compared to over-the-top services.

Over-the-top service and content providers have been required to reduce the quality of video provided to subscribers, in order to reduce streaming bit-rates and ensure that essential lifeline services, as well as news and entertainment are provided to as many as possible[1].

In contrast, the traditional, dedicated-platform pay-TV services to which the Consultation Paper applies have not needed to ration services and have provided the same, consistent service quality during the Covid-19 response as they did before it.

[1] See, for example https://timesofindia.indiatimes.com/business/india-business/streaming-internet-cos-to-reduce-resolution/articleshow/74802120.cms, https://www.thehindu.com/news/national/telecom-operators-ask-over-the-top-media-services-to-reduce-video-quality/article31136171.ece and https://www.deccanherald.com/specials/google-netflixhotstar-tiktok-and-others-to-cease-hd-content-in-india-over-coronavirus-817539.html

The reason is that traditional, dedicated-platform pay-TV services do not “share” capacity with other essential services and use substantially the same bandwidth however many subscribers are using their services.

Synamedia urges TRAI therefore not to encumber the traditional, dedicated-platform pay-TV service providers with new regulatory hurdles, given their proven ability to provide consistent service quality in the most critical and trying circumstances.

Synamedia is pleased to provide its recommendations in its response to the consultation paper questions, including both upgrades to the existing Schedule III features and new features to add.

Please let the author know if TRAI needs any further details or clarifications on the features recommended by Synamedia or any other matters relating to this response.

Synamedia Responses to TRAI Consultation Paper Questions:

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?

Synamedia: While keeping all the features mentioned in Schedule III of TRAI Regulations, Synamedia recommends a number of additional features and also expanding some of the Schedule III features as described below.

The following features need to be included in any CAS solution.

Please note that the generic term “decoder” below includes all types of pay TV authorizable device including digital video recorder (DVR), integrated digital TV (IDTV), integrated receiver decoder (IRD) and set top box (STB).

Conditional Access Standards Compliance

1. Scrambling Method – DVB-CSA

Scrambling must comply with the DVB Common Scrambling Algorithm (CSA)

2. Head-end interfaces - DVB SimulCrypt

Compliant with Version 2 and Version 3 of the Simulcrypt specifications ETSI TS 103 197:

CAS system should comply with the DVB Simulcrypt model. The DVB Simulcrypt document (Head-end implementation of DVB SimulCrypt ETSI TS 103 197 V1.3.1 (2002-06)) specified some interfaces and protocols between various sub-systems. The two main interfaces are:-

a) EMMG to MUX

b) ECMG to SCS

Two more interfaces should be included:

a) EIS to SCS – CAS and compression vendors should have adopted the OpenCAS standard as defined in Headend implementation of OpenCAS SCTE DVS/278r1, Date of Issue: Nov.17, 1999 (Revised: July 31, 2000)

b) The interface between SMS and EMMG

3. Multi-layer IC technology on the smart card

Standard Security Features

4. Per subscription programme authorization

   Ensure decryption only for those authorized to one of the multiple unexpired programme services, which may apply to channels, sets of channels, programmes, or sets of programmes.

5. Disable/enable decoder

   Individual decoders or groups of decoders are prevented from descrambling any service, regardless of the authorizations stored in the smart card or other security device. (Or enabled to descramble any services, only on similar specific re-enabling.)

6. Disable/enable CAS agent

   Individual smart cards, or groups of smart cards (or other security devices), need to be capable of being disabled or enabled over-air.

7. Disable/enable programme service and possible automatic renewals

   Individual smart cards, or groups of CA agent need to be capable of being disabled or enabled over-air to decode any one particular programme service.

8. Disable/enable unique service for a-la-carte channels and possible automatic renewals

   Individual smart cards, or groups of CA agent need to be capable of being disabled or enabled over-air to decode all programmes on a single a-la-carte channel.

9. Support subscription access to programmes

   Individual smart cards, or groups of CA agent need to be capable of being enabled or disabled over-air to decode a set of programmes independent of the channel.

10. Support pay-per-view access to over-the-air programmes

    Whether purchased interactively via the decoder or purchased online from a website or directly from a sales associate.

    Upon purchase, programme can be viewed for its entire duration until expiration.

11. Support rental viewing model

    Upon purchase, a purchased programme/channel is available for a duration of time, starting from the first actual viewing.

12. Support of pre-paid model

    Upon pre-paid purchase of a token, a viewer can watch all channels relating to a programme service for a duration of time until expiration.

13. Support of Individual Free Preview

    In this model, a user without an entitlement can watch a programme for a limited period of time, this time is counted individually for each user, starting from the beginning of the actual viewing.

14. Support of pay-per-time viewing

    In this model, a user is allowed to view a programme/channel for an accumulative time counting only the actual viewing time. The user is billed post facto based on time watched.

15. Set/unset user/device profile

    For example, domestic subscriber or bar/club/restaurant subscriber.

16. Send immediate and persistent messages to decoder

    A text message is sent to individual decoders or groups of decoders for display on the screen; alternatively, the over-air message may comprise a display command and address of a message which is pre-stored in the decoder or smartcard, for example, to warn of imminent expiry or to request the viewer to contact the SMS because of account difficulties.

17. Send message to decoder for individual programme service

    A text message is sent to individual decoders or groups of decoders in the same way as above, but is displayed only when the decoder selects the relevant programme service.

18. Secure media pipeline

    Secure media pipeline where the content-encryption key is extracted, content is decrypted and decoded in a secure atomic fashion in secure hardware.

19. Secure bootloader authentication of all software

    Secure Bootloader authentication of all software at the time of download and at each boot using asymmetric security based on the root of trust.

20. Secure installation and storage of root of trust in decoder

    Must be tamper-proof and not accessible by human hands. All secure functions must be performed only in the Trusted Execution Environment established using this root of trust.

21. Electronic countermeasures

    CAS must incorporate an extensive range of countermeasures. In order to combat hackers, CAS vendor should have a robust set of electronic and other countermeasures.

22. Changing content encryption keys

    Encryption keys should be configurable to change every N seconds for broadcast content. (For example N=10 seconds.)

23. Disable device or card-based Encryption keys

    Disable device or card based on suspicious activity indicative of service theft.

24. Secure Subscriber interface communication link

    The interface between SMS and CAS should be protected. The Subscriber Management System (SMS) should be connected to the CAS headend using a secured TCP/IP connection.

25. Persistent protection of locally stored content for DVR

    In the case of DVR, all content stored on the hard disk or other local storage should be secured by deployed CAS. All content stored in hard disk or other local storage needs to secured with the same level of encryption as a broadcast channel. This prevents copying of content between hard disks or other local storage, as the content will only be permitted to be decrypted in the DVR it was originally recorded on.

26. Entitle DVR to record and playback content

    DVR playback for all authorized to the recorded asset only. Ensure decryption on DVR on playback for those authorized to the recorded asset only.

27. Parental rating controls per programme

    Programmes can be rated according to content and Parents can easily block their children from viewing inappropriate or offensive programming by PIN control.

28. Channel blocking

    Channels can be blocked at user discretion.

29. Addressable blackout

    Blackout on all addressing criteria including region, time, service and postal / zip code. CAS must support regional blackout as well as spot – allow particular viewers in a blackout region to view.

30. Broadcast mail (B-Mail) and on screen display (OSD) messaging

    a) B-Mail: Using this mechanism, SMS may direct a message to the customer's decoder, such as a billing reminder, notification of an unpaid account, or even to send birthday greetings. The message may be deemed urgent or non-urgent, and the subscriber may or may not be allowed to delete it. B-Mail messages can be sent addressed to a single subscriber or groups of subscribers.

    b) OSD: Direct a message to a subscriber or group(s) of subscribers that will trigger the display of a text box overlaying the video screen. The text box may contain any free text in any character set required by the broadcaster. The text is will be displayed for a given time as specified in the SMS message. After the message has been displayed for the pre-set time, it will disappear and not return.

31. Subscriber entitlement management in a blackout region

    CAS must support the management of subscriber entitlements.

32. CAS product and version proposed to Indian Operators should not have any history of hacking in India or other worldwide locations.

33. PIN/Password protection

    Subscribers can restrict access to programmes and system settings with a password

34. Unique algorithm per operator

    To avoid piracy, CAS solution provided to every operator should have a unique algorithm.

35. Control word encryption

    The CAS Should support Control Word Encryption

36. Flexible subscriber addressing mode (General, Unique, Group, Logical)

    All modes should be supported as standard. CAS system should be very flexible in the ways that messages and actions can be addressed to subscribers. It should allow the targeting of messages, actions, and entitlements to view in a very flexible manner.

37. Custom-design smartcard per each operator

    Each broadcasters smartcard is unique, and each broadcaster's secrets are unique.

38. Display customer's card ID upon a command sent over-the-air, or by user

    The serial number of the smart card, or other means of unique identification (ID), is displayed on the screen. This is not the secret ID contained within the card, but is an unprotected ID which could be printed on the card. This function is useful for maintenance and other security procedures.

39. Emergency Message

    Deliver and display an emergency message in near real-time independent of tuning state of a particular decoder

40. Display a-la-carte price on present/following programme banner and in programme guide

Anti-piracy measures

41. Overt and covert fingerprinting

    Implement a comprehensive fingerprinting solution

    a) Overt fingerprinting – the fingerprint is visible to the viewer and can appear anywhere on the screen. The colour, duration, transparency, and position of the fingerprint can be varied by the operator by altering the parameters sent to trigger the display. In this method, the fingerprint is displayed on the viewing screen as a hexadecimal representation of the smart card number. The fingerprint can be targeted globally, addressed to subscribers watching a particular channel or service, or by any of the standard addressing methods.
    b) Covert fingerprinting – the fingerprint is embedded in a non-viewable portion of the video signal. Special software is required to decrypt the covert fingerprint. This type of fingerprint is usually used to target illegal copying and distribution of programme material. The fingerprint can be targeted globally, addressed to subscribers watching a particular channel or service, or by any of the standard addressing methods.

42. Decoder Pairing

    Decoder is hard-paired to the viewing card at subscriber activation time and control word encryption is used thereafter to secure the decoder – smart card interface. The CAS systems need to support the pairing of the smart card. Typically a broadcaster invokes pairing to prevent the smart card from being moved to another decoder

    a) Pairing needs to be robust in that it ensures that there is also a secret interchange between decoder and smart card using a secure secret sent from the headend at activation time. This close and secure relationship between decoder and smart card also means invoking of control word encryption where appropriate communications between the decoder and the smart card are encrypted using a secure method.
    b) The pairing relationship can be reset from the CAS head end in response to an SMS command.
    c) Pairing decoder and the smart card is an essential security feature to prevent the sharing of smart cards.

43. Taping control

    CAS must support taping and control formats (for example: HDCP).

Additional Features

44. Flexible pricing tiers

    CAS should allow tiering and packaging of services as standard

45. Number of subscribers supported with the CAS to be specified (With necessary HW and SW upgrades). The CAS system should be scalable with the addition of software or hardware to support the growth in subscribers.

46. Installations

    CAS products offered to Indian operators should have an International Installation base and acceptance.

47. Decoder integration

    CAS should have integrated with multiple decoders so that multiple decoders can be made available for Indian users.

48. Support

    CAS vendor needs to have appropriate support staff available in India to support Indian operators.

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?

Synamedia: Not all of the CAS solutions deployed comply to the required features as detailed in Schedule III, as is evident from the Consultation Paper. Many features are highly dependent on eco-system partners for compliance, including on-screen display (OSD), broadcast mail (B-Mail) and fingerprinting. The CAS needs to be very tightly integrated with Middleware (MW) for secure and reliable implementation of such features. In many cases there is no third-party MW in the STB and many basic jobs are fulfilled with STB native software of widely varying quality and security. As a result, such solutions may not comply to all the features mentioned in the requirement documents.

To check such compliance, every CAS should be certified by any international third-party content security expert body. These certifications should be renewed whenever any significant changes in the technology are introduced. Only such certified CAS should be allowed to operate in the Indian market.

Technical Audits must be carried out at each operator’s site by competent, qualified Technical personnel with specific CAS integration or operation experience. Only such real-world audits will enable thorough end-to-end system compliance verification of all the features deployed by each operator on the ground. In the case of MSOs running unified versions of CAS – SMS – MW – STB at more than one headend location, it **may** be possible to reduce the audit requirement to one of the deployed headends.

Synamedia also proposes and recommends an automated secure reporting mechanism to enable verification of transactional integrity between SMS and CAS. Synamedia will provide TRAI with detailed use cases for this for TRAI's and other stakeholders' consideration, but does not consider these appropriate for general publication at this stage.

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?

Synamedia: The basic requirements of CAS are covered in Schedule III of TRAI regulations.

CAS is a globally deployed technology, protecting content worth over one quarter of a trillion US dollars[2]. As innovatiions continue in all technology verticals, so they do in CAS. Synamedia believes that TRAI should continue to use Schedule III as-is for basic qualifying requirements for the CAS with added features at regular intervals to make it more robust and to accommodate new innovations in these regulations, rather than defining new CAS frameworks.

The requirements listed in the answer to Question 1. above should be the absolute minimum requirements required by all CAS solutions operating in India.

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?

Synamedia: In general, over-the-air (OTA) upgrade facility is a MUST have in any Pay TV Solution. CAS absolutely MUST support such upgrades. Must support targeted upgrade where nt all STBs are upgraded at once and ECM streams are backwards compatible to old CAS version while enabling new features in new CAS version

This should not be regarded as an issue. Neither subscribers nor operators, as principal stakeholders are suffering due to properly planned, tested, managed and implemented upgrades. In fact they are highly desirable for both parties. From the operator's point of view, they enable addition of improved security and new features, functionality and revenue generating opportunities on already deployed boxes. From the subscriber's point of view, they enable existing devices to receive new features, functionality and services not previously offered to the subscriber.

Of course, poorly planned, tested, managed and implemented upgrades may have distruptive consequences for operators and subscribers. The ability to roll back problematic upgrades promptly and the appropriate procedures to decide when to and how to achieve this with minimal disruption are part of best practice planning of such upgrades. Furthermore, the ability to upgrade and test a

[2] "The global pay TV market size was valued at USD 225.9 billion in 2019" https://www.grandviewresearch.com/industry-analysis/pay-television-tv-market

limited subset of the decoder population – after first testing in a lab environment for example – is also a MUST.

Synamedia thus strongly recommends that secure OTA upgrade be a mandatory qualifying requirement for all CAS, with ability to target subsets of the decoder population and ability to roll back changes rapidly in the event of unforeseen problems arising.

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.

Synamedia: At this stage, with digitalization completed across India and all the operators having selected and using their CAS solutions with more than 160M STB's / consumers deployed, Synamedia does not believe that this is an appropriate time to (re-)define the CAS Framework. However, additions to Schedule III are a MUST to make current deployed CAS systems more robust and hack-proof.

At present, globally almost all CAS vendors support the DVB-CSA, DVB Simulcrypt and other relevant DVB and ETSI standards. Synamedia recommends TRAI continue to follow these. New innovations are always in progress, including with CAS technologies, and new content delivery, integration and security features are being added and enhanced according to CAS vendors' roadmaps. Synamedia recommends to review and as necessary update Schedule III at predefined intervals – for example 18 months – to mandate new features and technological updates as MUST have requirements for any CAS systems currently deployed or to be deployed in India, and to add others to RECOMMENDED to have requirements.

Furthermore, Synamedia recommends that premium content providers should be permitted to require features, functionality, performance and security above the baseline MUST have requirements, but within the RECOMMENDED requirements for provision of niche content, exceptionally high value content (such as live pay-per-view sports events), HD content versus SD content, 4K content versus HD and SD content, DVR recordable content, multiple times rewatchable or permanent rights content delivered to DVR, and for other non-basic content delivery or usage options. Such differentiation is a feature of any healthy, innovating competitive market, and a healthy, innovating competitive market is the best guarantee of both value for money for subscribers and subscriber satisfaction over the long term.

Synamedia has recommended a comprehensive list of such features in its answers to Question 1.

(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.

Synamedia: Synamedia will provide its suggestions to TRAI privately.

Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.

Synamedia: Operators must first check whether the CAS solution(s) they are using comply with TRAI's currently mandated technical requirements. This is the responsibiiity of operator, but may need vendor cooperation.

Synamedia suggests a two-fold compliance mechanism, which may formalise existing practice.

Each CAS should be tested and audited wherever deployed, as explained in the answer to Q2. above. Furthermore, where the CAS have been proven to meet all the mandated minimum requirements, a separate type approval should be granted to the relevant vendors. This can be used to prove to other operators that are in the market for new CAS etc – whether for replacement of non-qualifying systems or for new operator installations. TRAI is not best placed to perform these tests, but can control the audit process by approving and periodically auditing the capabilities of the relevant auditing bodies.

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.

Synamedia: As mentioned previously, Technical Auditors should perform the relevant audits only at Operators' sites. Synamedia can and does work with a range of auditing and certification regimes from industry association led – for example CableLabs in US – to direct government agency led – for example in Peoples' Republic of China – with many intermediate options. Key criteria from Synamedia's point of view include:

1. Sufficiently qualified and resourced Technical Audit teams
2. Clear, fair, open, non-discriminatory and transparent criteria and process determination, preferably based on market-proven regimes
3. Clear, fair, open, non-discriminatory and transparent testing process and procedures, preferably based on market-proven regimes
4. Reasonable remediation timescales for small numbers of minor non-compliances – which may be caused by misunderstandings, differing interpretations, minor misconfigurations at time of tests etc
5. Emphasis on increasing quality of service experience for subscribers, including minimising any service disruptions, as well as on improving content security.

(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.

Synamedia: As mentioned above, this is not the appropriate time for considering the planning stage as almost all the operators have selected the CAS partners and have deployed more than 160 million set top boxes. It is not viable for them to re-invest in these soon.

Also it is important to note that CAS systems are following global standard of DVB-CSA throughout the world.

There is no need to develop India-specific separate standards, as now there is no large volume left that would justify for vendors' efforts to develop Indian-specific CAS products for. India should ride the global wave if it wants Indian subscribers to take the advantages of global technological developments. The global pay-TV market continues to change, with streaming video / OTT and hybrid subscriptions increasing.

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?

Synamedia: While it is understood that, CAS system deployed should comply to mandatory features considering the content security at highest level, in India, it is too late to discuss a new framework for CAS as almost all the Pay TV Operators have already selected the CAS partners and have deployed more than 160 million set top boxes.

It is required to inform operators to select appropriate CAS partners, whose products comply to all the mandatory requirements of CAS at a bare minimum, can protect the content with security at the highest standard today, and can demonstrate with a proven track record both the ability to provide, and actual timely provision of, technical upgrades, as well as credible roadmaps showing what they are already planning to offer in future updates or upgrades to the CAS. TRAI should give operators the opportunity to rectify any mistakes (if any) made earlier while selecting the partners. TRAI would thus need to discern and publish a phased manner approach for such operators to upgrade or replace the CAS systems so that the CAS they have comply to regulatory requirements.

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.

Synamedia: Standardization and certification of CAS may or may not bring about greater economic efficiency or customer experience overall, but it certainly should improve content security level to the minimum features and functionality required and recommended by TRAI.

If ONLY CAS which comply to TRAI requirements mentioned above are used, along with audited SMS – CAS throughout the Indian pay TV ecosystem, piracy and underreporting ought to be reduced and most legitimate operators would generate more revenue, increasing their cost efficiency and enabling broadcaster to invest in and provide further high quality content. Subscribers overall would benefit from improved content and and provide improved user experience. Government would benefit from increased tax revenues. Of course, some current subscribers that benefit from sub-standard SMS – CAS arrangements today to receive pay TV channels at lower than the correct tariffs, will need to pay more for legitimately distributed and priced content.

Q9. Any other issue relevant to the present consultation.

Synamedia: Synamedia also recommends the below features as listed below.

1. STB hardening
2. Tracking viewing

   CAS should allow using AMS (Audience measurement System), which can report back viewing habits to the headend for analysis. This is dependent upon a return path being available.

3. Open interface to third party head end platform

   For ease of integration.

Requirements pertaining to Compromise Recovery

4. Disable device or card based on suspicious activity indicative of service theft
5. Disable devices, deemed suspicious of content theft (HDCP bypass)

Requirements pertaining to Security of CA messages

6. Signed and Encrypted EMMs and ECMs

Requirements pertaining to Decoder Security

7. Secure channel between decoder and CAS agent to prevent snooping or modification of communication
8. Strong obfuscation of software
9. Non-cloneable security agents based on secure hardware
10. Zero-knowledge authentication of the smart card by the decoder

Contradictions inherent between current TRAI Schedule III Framework and recent TRAI Recommendation

It is unfortunate that, despite industry advice to the contrary, TRAI has recommended CI+ 2.0 support be mandated in all decoders, as per TRAI's Recommendation on Interoperability of Set-top Box published on 10 April 2020.

The CI+ 2.0 standard, while addressing many of the weaknesses inherent in earlier CI standards, fails to address a number of the requirements that TRAI has already acknowledged in Schedule III as minimum requirements for security. These failures include lack of standardised support for covert fingerprinting, for example. The recommendation thus represents a step backwards in content protection and regularisation of the Indian pay-TV market, for no obvious gain, as no cost-benefit analysis has been performed and published to justify such an enormously disruptive requirement.

Citing Germany as a successful implementation of CI+ 2.0 (and such legacy CI standards as already deployed) fails to acknowledge that unauthorised redistribution piracy by licensed cable operators and underreporting of subscriber bases is not known to be an issue in the German market, which is also a very stable, high average-revenue-per-subscriber/unit (ARPU) market as compared to India.