NAGRA
KUDELSKI

Date: 3rd June 2020

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

Subject: Comments on 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.

Dear Sir,

At the outset, we would like to thank Telecom Regulatory Authority of India (TRAI) for giving us an opportunity to provide our comments regarding the Framework for Technical Compliance of CAS and SMS.

Please find enclosed our comments for your kind consideration.

Thanking You,
For Nagravision SA,

Philippe Stransky-Heilkron
Senior Vice President - Technology
Central Architecture Office

Comments from Nagravision SA

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?

Features of 1-way CAS based on different categories:

Security -

- Secure TEE based or Hardware root of trust based (security module) security for SoC integration, Pairing for protecting communication between the smartcard and the STB or for Cardless CAS and the STB. This secure channel must be implemented up to the descrambler in the SoC of the STB.
- Geographical Blackout (ability of the CAS to blackout a particular region based on Pin Codes if required by the Government agencies or for other reasons)
- Content Usage Control: recording control on local PVR and other content export mechanisms, including but not limited to control of HDCP, DTCP.
- The CAS software and the CAS database should be hosted on a separate physical hardware and such hardware cannot be used to host any other software such as SMS. A firewall should be configured between the CAS and the SMS.
- Log of transaction between the CAS and the SMS.
- Export of the state of the CAS database for reconciliation with the SMS database.
- Firewall – Access to CAS systems should be allowed only through a Firewall.
- Parental Control: Parental Control (Maturity Rating) is a content specific setting specifying the minimum audience age the content is considered suitable for. It is a feature enabling consumers to block access to offensive content.

Anti-Piracy

- Revocation (blacklist) of STB and/or smartcard: the CAS is not able to generate any EMM addressed to a STB or smartcard that is revoked. This is needed in the case where STB and/or smartcard has been stolen, disappeared from the inventory or has been cloned.

- Covert Forensic Watermarking – The ability of the CAS client to insert a hidden watermark in order to identify a particular STB involved in piracy and distribution of pirate signals by detecting illegal distribution and tracking of the sources of the original content. The covert Forensic Watermarking should be resilient to noise, cropping of image, reduction in resolution and collusion. The solution should allow a pirated video clip to be uploaded in an automatic detection tool to identify the watermark and hence the pirate STB to immediately take the necessary action.
- Overt fingerprinting (This fingerprint is visible on the video screen and has limited ability to prevent piracy and the distribution of pirate signals)
- Covert Fingerprinting (This fingerprint is not visible on the video screen but again limited to prevent piracy and the distribution of pirate signals)

General Operations / Ease of Operations

- EMM addressability: Unique (sent to a particular subscriber), Shared (sent to a group of subscribers) and Global EMMs (sent to all subscribers) should be available, allowing optimization of the addressability of subscribers in a timely manner. Subscription with automatic expiration. The expiration date controlled by the CAS is shorter than the end of the subscription period granted by the SMS to the subscriber. The expiration date is extended by the CAS automatically at regular intervals until the end of the period purchased by the subscriber.This enables flexible management of the entitlements. For example, it avoids the need for negative addressing, i.e. the need for sending a subscription cancellation EMM at the end of the subscription period.
- A-la-carte subscription to support atleast 1000 channels
- Messaging – enables Operators to send a short, alphanumeric message to one or more subscribers (sent to and displayed on-screen by their STBs).
- Pay Per View – This feature enables operator to sell access to a content for limited period of time.
- On-demand – Option to sell access to content, such as movies, when requested by the customer (video on demand)
- EMM Pull (need to explain) - Primarily meant for two-way IPTV network where the device can contact backend over HTTP interface and retrieve all EMMs addressed to it over HTTP.
- Voucher - To provide access through vouchers for a set of content depending on the limit of Voucher.

Features of 2-way CAS:

A 2-way CAS required for IPTV or OTT STBs should also support the above features.

Features of DRM:

A DRM should also have the ability to support a subset of above features.

A CAS vendor should support 1-way CAS, 2-way CAS and DRM.

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?

We believe that a certificate from CAS & SMS vendor is sufficient to confirm the compliance.

While we are not aware of the compliance to the audit procedure by other CAS & SMS vendors, we strongly believe that a compliance certificate certifying that the SoC (System on Chip) has implemented secure TEE or hardware root of trust (security module) needs to be issued by the SoC vendor. This is absolutely critical because the entire security workflow is dependent on the SoC. This should be an additional certificate.

In addition, support from SoC vendors is required on a regular basis for updates of security patches, updates of SoC drivers etc. and hence it is important that the SoC vendors have a registered office in India with the necessary infrastructure to provide 24 x 7 support.

Further, with reference to the recent STB interoperability recommendations, even the DVB USB 2.0 CAM vendors should have a registered office in India with the necessary infrastructure to provide 24 x 7 support.

Further, even the CAS and the SMS vendors should have a registered office in India with the necessary infrastructure to provide 24 x 7 support.

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?

Kudelski Group CAS (both Nagra and Conax) comply to the DVB Standards for deployments in India region.

Excerpt from the DVB- ETSI EN 302 307

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital *television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardization, interoperability and future proof specifications.*

While we follow the DVB standards, we also agree that there is a need to define a framework for the overall Digital TV systems in India. There is a need to define CAS security and robustness to ensure that the business and technical interests of Operators and the Government of India are fully met.

Movie content providers (for example Hollywood studios) require the operators to implement specific technical, security and organizational measures, from content handling by the operator to content transmission to the subscribers. These measures are documented in various documents published by studios (for example MovieLabs ECP specification, MPAA Best Practices Common Guidelines, etc). MPAA has also introduced an audit and certification procedure program: Trusted Partner Network (TPN: www.ttpn.org).

These guidelines help operators to evaluate if the CAS and SMS products are compliant with various security measures, including but not limited to cybersecurity requirements.

Furthermore, and although there is currently no official equivalent consolidated and approved set of measures defined by the broadcast industry, that would apply to linear broadcast and live broadcast of sports events, Nagra has been working proactively on the matter and proposed a specific profile of the MovieLabs ECP specification targeting broadcast services, that includes additional requirements that expand on the Enhanced Content Protection requirements, to better cover security issues related to broadcast TV services, such as enforcement of a secure chain of trust or more advanced cryptographic and hardware security mechanism to better manage control word and right security.

Some sports content providers have defined similar additional measures and there are discussions in the broadcast industry to achieve some form of consolidation. The European Broadcasting Union (EBU) has also created a working group for infrastructure security and media cybersecurity (tech.ebu.ch) and has already published some security recommendations to its members.

We are willing to participate in the process and share inputs to ensure that a strong framework is defined and published.

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?

Upgrades are an integral part of the software solutions to ensure latest features, content security and cybersecurity requirements. At Nagra, we try to limit the number of upgrades for our CAS systems to a minimal level. But in order to support requirements by our customers and to update the security levels, upgrades are scheduled accordingly, taking into account the need for avoiding any service interruption, including the management of subscriptions and support to subscribers.

Also, to be noted is the fact that the Nagra upgrades are limited only to core systems and does not impact the data values or logs available for reporting architecture. In fact, in some cases the upgrades have been done to suffice the requirements defined by TRAI for audit features.

As mentioned earlier, in order to safeguard the consumers and the stakeholders, it is important that all partners involved in the value chain i.e. SoC provider, STB provider, CAS provider and SMS provider should have a registered office in India with 24 x 7 support.

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.

We propose that TRAI leads the overall monitoring and execution with support from BIS (Bureau of Indian Standards). Assign industry members including the leading CAS vendors, Operators and SMS vendors as part of a group to define the framework.

As TRAI is the leading authority that defines the rules and regulations for the industry, and therefore is in best position to ensure proper measures are put in place. Adding industry members will ensure that the operation and business interests are considered as part of the framework.

(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.

The below structure can be followed to achieve the required objective –

- TRAI to lead the overall process and organize a kick-off meeting with all parties
- Timelines and project plan to be defined in a follow up meeting
- Framework outline to be defined by TRAI (with support from BIS)
- Industry members to share additional inputs on the framework
- Industry members to provide supportive data and procedures based on global experience and existing frameworks available publicly
- TRAI, BIS and Industry members to jointly review the framework
- TRAI to release the framework for final review
- Industry members to provide final inputs on the framework
- Based on inputs, TRAI to publish the final framework document

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

The below model may be followed for the compliance mechanism

- TRAI to designate approved auditing companies, possibly Government agency (agencies), to carry out testing and certification.
  - For example, BECIL is already involved in audits and the role can be expanded.
- The compliance testing can be done once (not on an operator basis) and later as per recommendations from TRAI/BIS. It is recommended that the approved auditing companies have the flexibility to conduct such compliance audit on the available vendor sites in order to reduce the logistics and other costs of shifting hardware.

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.

There are examples of audits delegated to approved auditors, for example the Trusted Partner Network (www.ttpn.org) managed by movie content companies in the US. TRAI and the industry can setup a similar structure for India.
TRAI can obviously designate Government agency (agencies) to carry out testing and certification.

- BECIL is already involved in audits and the role can be extended for testing and certification of CAS.

(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?

A complete PayTV operation involves SMS, CAS, content security and cybersecurity. Each of these components already have well defined frameworks for content and operations security. Some work is needed to finalize a security framework for broadcast content but it can be easily derived from existing security requirements and from the Annex III of the Interconnection Regulation.

As explained in earlier comments, Nagra and Conax CAS follow DVB-Standards in India and these standards govern the physical and data layer of the distribution system. We recommend to put focus on enforcing a robust CAS providing strong content security and security monitoring, along with the capability of SMS and CAS to jointly be able to support the services to subscribers and operations of the security of the PayTV system..

By enforcing the use of a robust CAS, TRAI would also limit the risk of the SMS to implement only the features that are supported by a less robust CAS. This would avoid, for example, that a simulcrypt operation mixing a robust and a non-robust CAS sees the SMS implementing only the features of the less robust CAS, and therefore not taking benefit of all the features of the robust CAS.

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

There are two aspects on the oversight mechanism:

- Process –
    - This mainly involves designating approved auditing companies and/or an agency to carry out the compliance testing and certification.
    -
- Technical Steps –
    - The auditor must have technical understanding and tools to test and certify the compliance. Approved certification, like ISO 27001, must also be taken into account.
    - We are willing to share more details on the technical aspects around a robust SMS/CAS and the required tools.

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?

As part of existing process, BECIL and other designated agencies are auditing the requirements mentioned in Schedule-III.

In order to validate the compliance as per new process, TRAI can designate BECIL to carry out the testing and certify.

Like for other regulations, an adaptation period must be granted, giving sufficient time for PayTV operations to adapt to the new framework. During this period, voluntary audits can be conducted by these operators, which results can remain confidential to the operators.

If major non-compliance remain after this grace period, and in order to avoid unreasonable costs and discomfort of the subscribers, TRAI and the PayTV operator must agree on waivers, which should not be detrimental to the initial objective of the new framework and limited in time.

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.

Standardization and certification of a CAS, especially to define the robustness will definitely improve content security and reduce piracy for the industry and restore fair competition. It will also improve quality of products, for the benefit of the operators and subscribers. For example, it would avoid that vendors of non-robust technology deliver fragile products that cannot be maintained and must be replaced shortly after deployment, for technical or security reasons.
Key components like Covert Forensic Watermarking assisted with automatic detection tools, can further ensure that content can be traced for the illegal sources.

Q9. Any other issue relevant to the present consultation.

It would be beneficial for the PayTV industry in India to join an anti-piracy coalition, for example AVIA (avia.org), or content protection activities promoted also in India by the Motion Picture Association.
This allows operators, content providers, PayTV industry actors and regulators to join forces in identifying piracy threats, agreeing on remedies and defining communication strategies, including information campaigns.