Famework for Technical Compliance of Conditional Access System {CAS) and Subscriber Management Systems {SMS) for Broadcasting & Cable services

June 16th 2020

Broadcom Corporation Comments:
Please note that being an SoC company, comments from Broadcom are with specific SoC methodologies and features. The rest of the features we assume will be covered by CAS companies.

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?

Basic requirements include:
Strong Keyword Protection Algorithm
Secure Keyladder structure
EMM and EMC should be transmitted in a standardized methodology
Supporting SoC would have software and hardware root of trust for hybrid STB's.

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?

This relates to Q3 where we feel a minimum set of requirements is needed. If not many CAS will not have good security measures, and will be just a decryption mechanism that can easily be hacked. So

certificate from CAS/SMS vendor may not always work as this certificate can be obtained for a weak CAS that is hackable.

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?

Yes. A minimum set of requirements is necessary, to prevent substandard CAS systems. This also relates to where a certificate from CAS vendor is available but it may not meet a minimum set of requirements.

Q4. What safeguards are necessary so that consumers as well as other stake holders do not suffer for want of regular upgrade/ configuration by CAS/ SMSvendors?

For unidirectional content a strong CAS that requires less upgrades is preferable.
Issues will arise when STB's go to hybrid mode and use applications such as Android TV, some of which are in the market already. Need to ensure that Hybrid STB's cannot download unsecure applications. SoC vendors can provide bootloader flags which can then be used by operators to flag pirated content through such applications. We bring this up as there are already hybrid STB's in the market.

Q5. a)Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons there of. Describe the structure and functioning procedure of such entrusted entity.

We think CAS companies are in a better position to suggest this. A consortium of CAS and SoC companies could assist in formulating the definition of the framework and its execution, which can be eventually be accepted by TRAI.

Q5(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.

Basic mechanism should be that stakeholders who have CAS's deployed in India justify the performance of their CAS systems and suggest minimum requirements that need to be made to make systems secure. Not sure of any example as yet.

Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.
a)Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of testing and certification be entrusted with accredited testing labs empaneled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.

Designating an agency to carry out testing is a good idea. However the agency should only ensure that all minimum requirements and some other requirements in terms of CAS and SoC compliance are followed. Precaution should also be taken to ensure that SoC companies are fulfilling all CAS requirements in terms of security and architecture.

(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.

The precaution should be that in addition to standardization and certification of CAS and SMS, previous records of CAS performance should be taken into account. If there are existing CAS's that are known to be hacked, they should explain how they are overcoming it. There should be also precaution taken to not allow CAS's that can be cloned among SoC's without proper licensing. This will need to be

taken up with Operators and CAS companies with SoC companies participating in securing CAS authenticity.

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?

Yes, existing CAS/SMS systems need to conform to the framework. Not being a CAS company we cannot comment on timelines. However our opinion is that a strong CAS is needed with a strong SoC supporting all 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.

Standardization of CAS and SMS will definitely be beneficial as there will be a minimum requirement set that will not allow sub-standard CAS's to flood the market. This will definitely benefit content providers and hence operators who will see a better revenue stream and hence bring economic efficiency through lower pricing and better features.

Q9. Any other issue relevant to the present consultation.

Apart from CAS security, nowadays SoC providers have envisaged additional security measures for content protection. The main features used are Hardware root of trust and Secure video path. We give a short descriptions below.

Many STB's are now in hybrid mode. They are both having traditional broadcast and OTT content. With this in mind, in addition to software root of trust envisaged by ARM Trustzone etc., Hardware root of trust is the foundation on which all secure operations of a STB/video decoder depend. It contains the keys used for cryptographic functions

and enables a secure boot process. It is inherently trusted, and therefore must be secure by design. The most secure implementation of a root of trust is in hardware making it immune from malware attacks. As such, it can be a stand-alone security module or implemented as security module within a processor or system on chip (SoC). The implementation within the SoC provides the highest level of security.

Secure video path (SVP) secures the entire video pipeline including the compressed and decoded data buffers for the high value video content. These video buffers cannot be accessed by a host application processor or any other non-secure memory client. This enables high value content to be fully protected as per the specs of movie labs. Rampant piracy in the STB and OTT space for premium content needs a hardened secure path to ensure rogue applications operating within the kernel space are also not allowed to access the secure path. However this SVP is for 4K video currently, and will be more popular in hybrid STB's.