25th August, 2017

By Email and hand

Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawaharlal Nehru Marg (Old Minto Road)
New Delhi - 110002

Subject: **Response to the Consultation Note on Solution Architecture for Technical Interoperable Set Top Box dated 11th August, 2017**

Kind Attn: **Shri Sunil Kumar Singhal, Advisor (B&CS)**

Dear Sir,

We thank the TRAI for this opportunity to express our views on the above captioned consultation note. Tata Sky's response to the same is attached for your ready reference.

Yours faithfully,

Manish Gupta
Vice President – Regulatory Affairs

Encl.: As above

Tata Sky Ltd.
Regional Office North : Tata Communications Complex, Mandi Road, PO Chhattarpur, New Delhi-110074, India.
Tel.: +91-11-66163000, Fax : +91-11-66163030
Registered Office : 3rd Floor, C-1, Wadia International Centre (Bombay Dyeing), Pandurang Budhkar Marg, Worli, Mumbai - 400025, India.
Tel. : +91-22-66133000, Fax : +91-22-66133030, CIN: U9210MH2001PLC130365, E-mail : contact@tatasky.com , Website: www.tatasky.com

TATA SKY'S RESPONSE TO THE CONSULTATION NOTE ON SOLUTION ARCHITECTURE FOR TECHNICAL INTEROPERABLE SET TOP BOX DATED 11TH AUGUST, 2017

Further to the meeting organized by the TRAI in its Bengaluru office on 10th July, 2017 in which M/s C-DOT had given a presentation on the above subject, we had submitted our comments vide our letter dated 8th August, 2017 ('Letter'). We request you to kindly consider the inputs in the Letter as part of our response to this consultation note. In addition, we wish to submit the following comments:

- The framework assumes that all CAS functionality can be pushed into a smartcard. For security, cost and operational reasons the industry trend is to push some or all functionality of a Conditional Access System (CAS) into the Set Top Box (STB). This trend started in the early 2000s and has accelerated in recent times as the main security threats have evolved to become illegal content and Control Word distribution. This has required new CAS techniques that cannot be applied outside the secure silicon that includes the descrambler block. These developments have enabled cardless CAS, which is not provided for by the framework.

- The proposed framework describes a means of communicating between two trusted parties, each having access to keys that they wish to maintain secret. Unfortunately, the two parties in this application could be in the hands of hackers. Experience has shown that hiding keys in secure memory is not sufficient, so many proprietary methods, often using dedicated hardware, have been developed to ensure that control words are protected against the most sophisticated attacks. The framework excludes the use of this hardware and firmware in security processors that would normally be used by Conditional Access Systems.

- The framework does not describe how responsibility for security of the STB and management of the systems will be performed.

- The discovery of Control Words, directly or indirectly, from one poorly implemented STB or family of STBs could compromise every operator (DPO) by enabling Control Word sharing or implementation of STBs that do not enforce copy protection and other CAS features that should be included in the STB.

- The threat model for a one-way broadcast system differs significantly from any connected service and broadcasting services have different threats to video on demand services, so a comparison with mobile phones cannot be made. For example, no single key can be taken from one phone and used to deliver the same service to all other phones. Additionally, mobile phones are high-end devices with software and hardware capabilities that are not available in set top boxes, unless one capable of supporting Android TV for example is specified. For this reason, UI and EPG are normally implemented in native code, which means a full software update would be required when STBs are ported between operators (DPOs). The bandwidth overhead may become unmanageable.

- CAS is not simply the application of cryptography in a solution design, the implementation of which is also an important issue. The need to hide secrets in use within an STB in the hostile domain requires the use of sound cryptography as well as obscurity through complexity of the hardware and software design as well as good design. Standard algorithms have their place in modern CAS design but variants and specially tailored algorithms implemented in hardware and or the use of data obfuscation and white box cryptography have many useful applications in STB and CAS design.

- There is inadequate information regarding the secure implementation or operation of a CAS in the proposed framework. This is in part because of the assumption that the CAS will be provided in a smartcard but it is unable to recognize the full functionality provided by a CAS and the need to provide a secure environment for processing the Control Word in the CAS along with a secure content path.

- There is inadequate information on how Control Word sharing or content protection might be protected against while in use within the STB, especially where the elements are included in the STB for both smartcard and cardless solutions. The CAS must include a secure content path as well as secure key management.

- The framework does not consider for future use any form of TEE which is an essential part of enabling a secure content path in the STB. This requirement is relatively new and is an example of how innovation must be allowed in the development, choice and implementation of SoCs and supporting software at least for future STBs as illegal content sharing becomes a more significant issue for operators.

- The framework does not describe to support CAS functionality such as on-screen subscriber ID display, overt and covert watermarking, the management of STB outputs and other copy protection methods normally controlled by the CAS.

- Commercial responsibility and liability have not been considered. The framework does not consider commercial responsibility for managing piracy. The CAS is not just a technology but an end-to-end solution that is often offered with security warranties and acceptance of liability by the CAS vendor. These liabilities provide protection against not only a design failure but an implementation failure and may cover even the cost of replacement of a smartcard or STB, or at least the software and firmware in the STB. New conditional access systems include significant Intellectual Property (IP). Recently, the level of activity in this area has increased with many new licensing schemes being announced, as new IPR has been deployed to enable cardless CAS and prevention of content and Control Word sharing. The proposers of any standardized design, let alone implementation, must address commercial liability for piracy and infringement of intellectual property or ensure proper licensing of the technologies used. The proposed solution does not address commercial liability or Intellectual property. Whilst the proposed scheme does not appear to include much IPR that might need to be licensed from 3rd parties this only reflects the lack of security functionality provided by the scheme when compared to a modern CAS.

- Also, Security of the system if now shared amongst multi parties, in case of a security breach is a sensitive and complicated subject, which will also have onerous legal and financial implications

- TA adds to an additional layer of complexity for any operational system. Irrespective of central TA, each operator or CAS provider may still need their own TA to suit operating environment. It is not clear on how STB manufacturers and operators will protect their secret code received from TA. The framework needs to consider the extent of the tasks and cost of running the TA and where the necessary skills can be acquired.

- The framework includes a certifying body but does not provide information on how this would be funded and resourced with the necessary skills to test and certify systems, which if done properly will be costly to establish and like any good review process will rely on 3rd parties to provide independent peer review, introducing many of the cost elements associated with CAS.

- The necessary technology and services would have to be developed for the STB components and would have to have all the necessary functionality to support multiple possible connected CAS. It is not clear whether the 'Test and Certification' will be undertaken by an authority and would that authority accept liability for the security of the solution.

- The video should be protected against content sharing. Each operator will have their own requirements or those imposed by the studios, the most onerous of which are the security requirements of Hollywood content providers. Content providers' views would be of considerable significance to enable premium content. We would request the regulator to officially include them in this consultation process.

1.1 The framework increases cost factors to a great extent

- The proposal does not clarify how universal interoperable STB will cover Satellite/DTH, Cable, IPTV, SD, HD etc. Cost increase will be significant as today's products are highly optimized for one specific market
- Security review and penetration testing the design and each implementation of STB and CAS combination will add significantly to the costs of the proposed framework compared to the existing environment.
- Requires high-end SoC to support PKI infrastructure, Limits choice of SoC, CAS
- Requires non-standard implementation of every CAS, including special smartcards.
- Highly customized STB and smart-card software, as highlighted in the proposal will further add to the cost. The earlier CAM solution and now even the smart-card based solution is not cost effective. Cardless STB is the only future.
- Requires smartcards and prevents use of cardless systems. Smartcards, if used at all, will require custom development for this market as the STB interface will not be standard for any of the CAS vendors. This will increase the smartcard cost for every operator as well as increase the risk of piracy for all.
- Custom STB software will be required
- The STB will have to be certified by every CAS vendor and each time a core software update is required will have to be certified by all the CAS vendors. In addition, a process will have to be developed to ensure that only software that is certified by all the CAS vendors is deployed. The framework does not provide for this.
- The STB or CAS vendors will have to purchase bandwidth on each broadcast system for each of the STB/CAS variants that they are supporting. The cost of this will be increased because all STB types must be supported on all platforms.
- Simulcast of messaging and security for legacy and highend STBs could incur a large overhead of bandwidth on already saturated transponders. Most of the providers do this through compressed SI which is proprietary in nature, however saves significant bandwidth as compared to standard DVB-SI.
- Software updates will have to be broadcast by all operators for all STB types at a high data rate to support the customers switching between operators. The bandwidth will be required even if a small number of subscribers move between operators. The need to support a branded UI and EPG, making use of rich meta data, would be one of the key reasons for requiring a software update & additional bandwidth will be required to support diverse STBs.
- **The existing approved CAS in market have been subject to rigorous design reviews of hardware and software, penetration testing of components and end-to-end implementation over years by approved third parties certified security agencies, existing C-DOT framework review for any possible implementation will add significant cost and time.**

1.2 The framework is unable to ensure security:

- The Control Word is protected only by a session key K, which is dependent on the secrecy of STB_{sk}
- The best CAS cannot be implemented due to a dependence on hardware in the SoC.
- The SoC represents the most significant component of the solution. Proprietary elements of the SoC are used to create secure smartcard solutions as well as cardless solutions. The choice of SoC has major impact on functionality, reliability and security yet this is no longer within the operator or CAS provider's control under the proposed framework, meaning the framework cannot be used by a secure CAS.
- The framework does not state how each SoC will be certified or programmed at time of manufacture, which is a requirement for most CAS. **The final specification, certification and security validation of each SoC will have to consider the requirements of each CAS currently available and future CAS as the security threat models and responses evolve.**
- There is no process for managing firmware changes in the security processors, as required to support CAS porting, security and maintenance.

- Provides single point of attack, the abstraction layer.
- Loss of a single key could compromise the system for all operators for all time if the key is only used to decrypt Control Words. Cloned STBs will be hard to detect and differentiate from the real STBs.
- Revocation of keys, meaning turning off subscribers' STBs may be illegal or so undesirable that it cannot be done (common experience).
- Depending on registration processes it may be possible to use one key with many operators.
- Once a means of getting one key from one STB is found it may be easy to replicate so shutting down single keys may not have any value.

1.3 The framework is not fully specified :

- No certification, security validation processes for STB or CAS using the interface.
- No liability and authority commercially able to provide warranties and undertakings.
- There is an IPR risk in its implementation.
- There is no revocation of keys.
- PKI layers required for programming of STBs/SoCs are not yet defined.
- There is no specification of overt (on screen subscriber display) and covert watermarking. Overt watermarking is a crucial mechanism as first defence against content redistribution.
- The security infrastructure is not yet defined.
- It is not clear how STB ID with respect to CAS will be maintained, which is flashed through serialization process at production.
- Control Word protection from the smartcard, traditionally a CAS role, is supplanted by this scheme in a way that is not properly defined and potentially unsafe.
- Customer support (e.g. management of failed activations), which is not needed for free to air STBs, is a core part of a pay TV service offering. The UI and the menus within this are critical to good customer care and must therefore be appropriate for each operator's customer care processes. In the absence of customer care by the operators none is specified nor can it be provided by the STB manufacturers.
- Not clear if the STB manufacturers be required to develop more of the components themselves and would they be required to underwrite the security of the solution as well
- There is no explicit deregistration mechanism, and no way for an operator to have knowledge that a subscriber's STB has joined another network

1.4 The framework restricts innovation:

- Does not allow innovation within the STB. The flexibility provided by the existing standards environment has allowed the market to develop, with competitive supply of CAS and STBs over the full history of digital television. The rapid emergence of new technologies to support Control Word and content sharing, and the adoption of cardless CAS have all been enabled by this flexibility. With prescriptive solutions, the industry would have required new standards, with slow development and a lack of innovation leading to higher STB prices and continued piracy problems.
- Forces a single lowest common denominator standard within the STB.
- Restricts smartcard communication to the simplest protection of the CW, use of a session key, dependent on a single private key, a method that has been in use since early 2000's and superseded in the best systems.
- Efficient addressing of smartcards is a key feature of a good CAS, but every CAS would have to be re-designed to use the inefficient Gn scheme to support the framework.

1.5 Additionally :

➢ We are not aware of any references that provide for a generic interface to any operator's smart-card. Supporting multiple CAS in one STB restricts the choice of CAS and SoCs that can be supported.

Certainly, not all CAS can be supported by all SoCs, even without the complexity of supporting multiple CAS in each SoC.

- As per the requirement of the proposed framework, all the functionality required to implement each interoperable CAS would have to be included in every STB or supported as a software download. This may not be practical for the secure firmware of the SoC and certainly not for any SoC hardware, which would have to be present in every SoC and correctly configured for each supported CAS. This makes the framework shown impossible to implement. Significant, out of the way implementation, might mean restricted CAS, would stifle innovation and increase costs through lack of competition and testing overheads.

- The framework gives the STB manufacturer ownership of the root secure boot signing key. Usually, this would only be acceptable to a CAS vendor where the CAS vendor has performed a thorough review and even penetration test of the proposed bootloader, which necessarily narrows the choice of STB vendors to those in the Tier 1 CAS space

- Managing the STBs is essential for delivering a reliable service to customers. Software and security updates are mandatory for each STB and are currently managed by operator as it is under their full control. In the proposed framework, such updates will be practically unmanageable.

- Managing middleware is a complex issue and maintaining many different software variants will be complex and potentially unworkable with inevitable operational and security consequences.

- There are several operational issues which remain unaddressed in this proposed framework, such as incompatibility of STB memory for different SoC, difference in transmission even inside DTH which require different STBs have licensed technologies like DOLBY, Macrovision, HDCP (keys need to be in STB), DRMs, codecs..

- For unmanaged STBs, failure to support an update to an STB, which may happen if manufacturer go out of business or have no revenue stream to support the upgrade, the STB will be rendered obsolete.

- STB Hardware/STB Quality - Operators currently have their own hardware and quality specifications, testing, verifications and hardware security verification as it is prone to hacking from PCB traces. The proposed framework does not address this. Will Reduce STB lifetime as STB manufacturers cannot be relied on to support products without commercial incentive to do so & Operators refurbish and recycle STBs to make the most of their capital investment, resulting in long STB lifetimes compared to other consumer electronics.

In absence of any defined standard and this proposed framework still being very high (macro) level, further detailing is required for each aspect of the proposed interoperable STB including security aspects of the end-to-end solution and responsibilities of each stakeholder.