Centre for Development of Telematics (C-DOT) Responses to TRAI consultation Paper on Set Top Box (STB) interoperability dated 11th November 2019

C-DOT, Centre for Development of Telematics, is India's premier telecommunication R&D Centre, has been a pioneer and a Nation builder, committed to providing a wide range of indigenously developed, cost-effective, state-of-the-art total telecom and strategic solutions and services since its inception. C-DOT has designed developed STBs for various segments with indigenously developed and tested State-f-the-art Conditional Access System (CAS).

C-DOT has been working as knowledge partner to TRAI for STB interoperability. Subsequent to the release of consultation paper by TRAI based on C-DOT solution architecture (https://main.trai.gov.in/sites/default/files/Consultation_note_on_STB_interoperability_110817.pdf) during August 2017, C-DOT had fine-tuned few details and clarified all the technical issues raised by the stakeholders during the TRAI workshop held during September 2017 in New Delhi. The details of the technical clarifications are also shared with TRAI. Below are some of the points w.r.t C-DOT solution architecture (latest version) & technical clarifications on STB interoperability those are reproduced herewith again (in Section I) for ease of understanding and clarity in this context. Section II gives C-DOT responses to the queries mentioned in the TRAI consultation paper dated 11th November 2019.

SECTION I (Technical points w.r.t C-DOT Solution Architecture)

1. Secure handling of Control Word (CW) in the framework:

The framework for interoperable STB details the functional requirements and provides an architectural illustration for achieving STB interoperability and achieving content/key security.

The framework details the mechanism of key/CW handling in a secure manner (Pl. refer to the figure 1 below) in STB & Smart Card (SC) and also in the communication path between them. The functional requirements are accomplished by usage of either Hardware Blocks or by a security processor / co-processor which is totally isolated from the application processor

of the SoC. The framework is agnostic to exact (technology parameters) low level security implementation specifics of Hardware / Software. As an example, for hardware modules to achieve anti-tampering requirements, either PUF (Physically Uncloneable Function) and / or any other technology can be used. Also within PUF, there are SRAM based PUF, Butterfly PUF, DRAM PUF, Strong PUF, Week PUF etc. The framework does not specify any of such low level mechanisms and is totally unbiased, agnostic and accommodative to any low level technology implementations. Similarly other mechanisms like, bus scrambling, active shielding, anti-DPA methods can be used and adopted as per technology & industry trend without impacting any interoperability requirements.

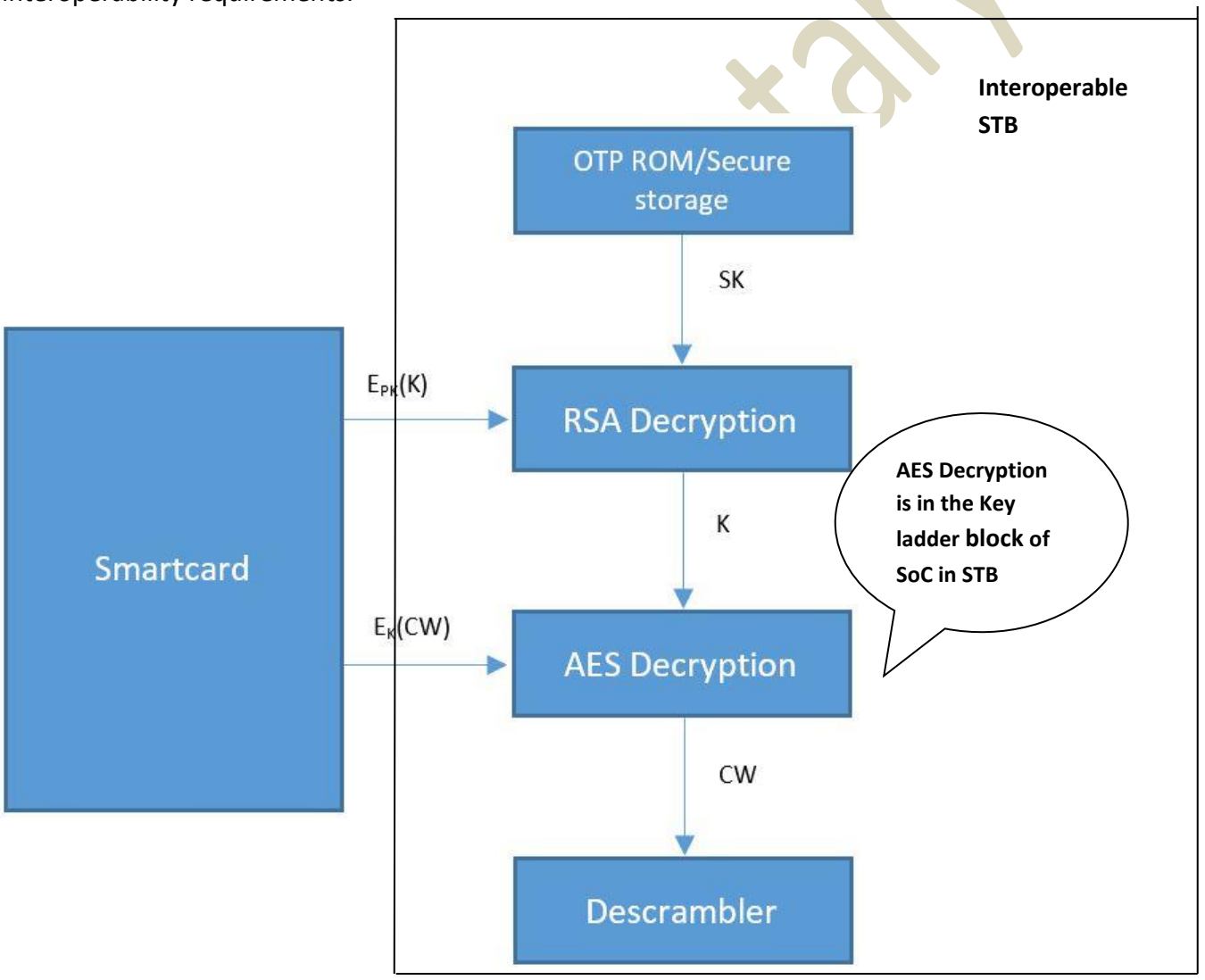

Fig 1

SK is RSA-2048 private key of STB.

PK is RSA-2048 public key of STB.

K is AES-128 symmetric key which is a dynamic and changes at every power up session of STB.

$E_{PK}(K)$ is RSA-2048 encrypted K using public key PK (encryption carried out in smartcard).

$E_K(CW)$ is AES-128 encrypted CW using K in smartcard (encryption carried out in smartcard) and it is decrypted in STB using Key ladder block of SoC. **CW and any intermediate keys, in clear form, is never available in the RAM of STB or in any other inside/outside interfaces of STB.**

a. From security point of view, SK (private key of STB), K and CW should not go to external RAM.
b. SK should be stored in secure memory of STB (un-modifiable and can be read only through Hardware/secure processor).

It is to be noted here that, in this solution architecture as well, Key ladder inside the SoC can be used; but here the Key ladder is not CAS specific rather a generic one and is used differently in this use-case.

C-DOT has designed and developed prototypes, meeting the requirements of C-DOT solution architecture for STB interoperability. It is to be noted that, although the requirements are implemented by C-DOT in a particular way/method/design as part of reference implementation (meeting all the requirements of the C-DOT solution architecture), C-DOT solution architecture does no way limit alternate physical implementations of these requirements by the relevant stakeholders such as SoC vendor, STB design houses etc.

2. Proprietary Vs Standard Based Solution:

In cryptology, standard based algorithms/solutions are always considered to be more secure compared to proprietary algorithms, as per two very fundamental principles of modern cryptography:

a. Kerckhoff's Principle

b. Shannon's Maxim Theory

i. There are many classic examples of these principles in recent implementations in the given context as well. It is a well-known fact that the industry standard algorithms undergo much more rigorous testing than most of the proprietary algorithms/systems. In fact, there are open challenges/competitions held and huge prize money is offered to anyone in the world who can break an algorithm, before it becomes an industry standard algorithms. Further, so far as, correctness of implementation of these standard algorithms are concerned, there are certifications by NIST under Cryptographic Algorithm Validation Program (CAVP).

ii. On top of this, C-DOT interoperable framework provides the detail requirements to be met by various entities including SoC/STB towards achieving a very high level of security towards handling of keys/content.

iii. There will be compliance testing for all elements such as STB, Headend, Smart card etc, specification of which will be finalized by taking inputs from stakeholders.

iv. In the Key ladder specification, ETSI TS 103 162 and ETSI ECI specification (ETSI GS ECI) all the algorithms and functions are made public. In C-DOT interoperable framework, ECM/EMM internal processing functions are not defined and every CAS provider is given the flexibility.

Hence it goes beyond any doubt and can logically be concluded that, in STB interoperable framework, the whole security paradigm effectively passes through much more rigid security analysis and testing than any proprietary algorithms and this completely aligns with the fundamentals of cryptography along with flexibility and space for innovations to the stakeholders.

3. Smart Card form Factors

In order to better optimize on the STB size and cost, a smaller form factor (Same as SIM card form factor) can be used in this case as well.

4. Security Attacks, Solution and Recovery:

a) Smart Card:

i. SC can be shared with anyone for subscription sharing.

Solution: Though this attack does not have any impact on the security of overall system, the attack is mitigated using OTP based binding. When a shared SC is inserted in any other STB than the paired STB, user is asked to complete the OTP based registration process again to pair SC and STB. User with shared SC also needs to have possession of registered mobile number or atleast the OTP sent by operator. At a given time, only one STB can be paired with the Smart Card.

ii. Eavesdropping of SC-STB communication for tapping secret information:

Solution: All communications after Bidirectional authentication process are encrypted by session key. Hence eavesdropping after bidirectional authentication process is not useful unless attacker has the session key. Also session key is shared in encrypted form using public key of STB. Hence the eavesdropping during bidirectional authentication is also not useful unless attacker has the STB's private key.

iii. MITM (Man In The Middle) attack on SC-STB channel:

Solution: To succeed in MITM attack on SC-STB channel, a valid key pair and certificates of STB/SC are required. But the private keys of STB/SC are directly programmed in the secure memories of STB/SC. These memories are accessible only to the crypto-hardware/secure processor and no software path is available to obtain them using a software attack.

iv. SC cloning:

Solution: Any SC can be paired with only one STB at any point of time by the operator. If the user tries to use the cloned SC with a different STB, then that STB gets linked with the SC in operator's database. A new key will be generated during the OTP process if completed successfully. This key will be used to encrypt the subsequent user specific EMMs. This new key can be received only by the SC attached to the STB which is used for OTP process. Hence the original SC will not be able to decrypt the new EMMs. In this way, even after SC cloning, only one SC-STB pair will be successful in decoding services at any given point of time for a given subscribed user. If attacker is able to clone STB also (total cloning of STB is considered to be extremely difficult/near impossible as on date), then all SC-STB pairs are identical. But in order to complete OTP process, all pairs should be online at the same time and users of those pairs should get the OTP from the corresponding registered user. But some damage can still be reduced if time duration for accepting OTP from the user through IR remote is restricted to a small duration (example 2 minutes) which is sufficient for the registered user to enter it through remote after receiving. If

user fails to enter OTP in given time, STB removes the screen for accepting the OTP and instructs the user to send the new OTP request to the operator.

b) STB:

i. CW sharing:

Solution: The CW is sent to STB in encrypted form by SC. CW is encrypted with session key which is also shared with STB in encrypted form and requires STB's private key to decrypt it. STB's private key is stored in secure memory which can be accessed by only RSA hardware. Also output of RSA hardware i.e. session key is given to key input of AES hardware directly. The CW is decrypted by AES hardware whose output should be routed directly to the descrambler. The keyladder mechanism can be used for this purpose. Hence, the CW (in clear form) is never exposed to any software and doesn't come out of SOC.

c) SM (STB Manufacturer):

1. STB firmware tweaking by unauthorized developer:

Solution: The STB boot process should follow secure boot flow in which only the SM's authenticated firmware should be able to boot. If any unauthorised developer somehow tries to load any tweaked firmware, the STB can't boot with the new firmware since it will not have a valid signature from SM.

ii. STB firmware tweaking by unethical application developer of SM:

Solution: The application developer who develops the GUI or other STB functions which are not related to the security, cannot have the access to the secure information stored in the STB since the application CPU is not allowed to access the secure information. This feature has to be ensured in STB hardware architecture itself.

iii. Unethical security code developer of SM:

Solution: If the security code developer of SM tries to tweak the security related code (like bidirectional authentication or OTP process), there is no risk of leaking of keys since the decrypted keys are strictly prohibited from being routed to the RAM. All keys when needed are directly fed to the appropriate crypto hardware. Even if developer tries to modify the code to skip some steps from authentication/registration process, it will not work out since these processes are designed to strictly follow the same sequence of steps.

Also, SM does not have access to the private keys of STBs, private key is directly sent by CSTAM to Chip vendors for programming. So, misusing the key pair at the SM end is not possible. The SC communicating with STB will not allow STB to skip any step or change the sequence of steps.

iv. SOC design bug:

Solution: The SOC design must be certified as per the specified standard by the independent certifying agency. Hence the bugs in SOC design if any will be detected in time.

v. Leakage of STB key pair and certificate at SM end:

Solution: The STB key pair and certificate is used during the bidirectional authentication to establish the secure communication channel between SC and STB. The leaked keypair and corresponding certificate can be used to impersonate as an authentic STB and eavesdrop the communication between actual STB and the SC and get the CWs from the genuine/authentic SC. Also as mentioned, there should be an independent industrial body (CSTAM) to issue the STB key pairs according to the demand from the STB manufacturer. The key pairs and certificates should be securely obtained and programmed by the SOC manufacturer itself and SOCs should be given to the STB manufacturer after that. The private keys should be destroyed securely (through well-defined security mechanism) by SOC manufacturer and CSTAM immediately after their work is done. CSTAM / STB manufacturer should maintain the database of the STB-ID and corresponding public keys for operators to access. The STB should send its STB-ID to the SC after completion/somewhere during the authentication process. SC should store it in the persistent memory.

The part of the trigger message encrypted with the user key (UK) should also contain the STB-ID sent by the user for requesting OTP from the operator. Also the SC should verify this STB-ID with the one sent during the bidirectional authentication. This will ensure that only leaked key pair cannot be used for CW sharing.

d) Operator/CAS server:

i. Leakage of SC keypair and certificate:

Solution: The SC keypair and certificate is used during the bidirectional authentication only to establish the secure communication channel between SC and STB. The leaked keypair and certificate can be used to impersonate as an authentic SC and establish a

secure communication with STB. But processing of EMM/ECM can only take place in a genuine SC issued by the operator. The output of the ECM processing i.e. CWs are sent encrypted with the session key known to only genuine SC and the STB. Hence leaked SC keypair and certificate are useless.

Some recovery mechanisms:

i. Implementation of ECM and EMM processing modules should be such that some modifications (e.g. encryption methods) can be applied over the air in these modules to temporarily stop the security breach in some cases.

ii. Re-issuance of new smart cards in case of any major security in the operators network

It is pertinent to mention that, in case of cardless STBs are hacked, the full STB needs replacement which is a costly proposition.

Some recommendations: 1. All the STBs sold in the Indian market must be certified. Selling of Uncertified STB should be made illegal.

5. Card Vs Cardless STBs

There are STBs in the network of both types: Smart Card based and also cardless. As per available reports, smart card based STBs as on today is a higher than the cardless counterpart, although cardless STBs are also getting proliferated in the field. In a non-interoperable scenario, there are pros and cons of both the types. It is extremely important the view this point from the perspectives of Interoperability in the context of India's demography. In an interoperable scenario, it goes beyond any logical understanding that advantages of Smart Card based CAS/STB, clearly out performs the carless version, given the eco-system limitations as on date. However, with the maturity of interoperable regime, cardless versions can also be developed & proliferated.

After the hacking of analogue cable system in the 1970's, Pay TV industry shifted to smart card based system in late 1980's to provide better security. It had been a very successful technology since Pay TV industry prospered very rapidly after that. But in the rush to launch the service, often the initial smart cards were prone to security attacks due to improper implementations. During middle of last decade, due to increasing number of attacks on smart cards forced operators to look for other solutions and cardless CAS implementations got adapted in Pay TV industry. But in recent years, newer technologies

emerged in the smart cards which increased their security to much higher level. Especially, from around 2012 onwards, the PUF technology and other anti-tampering technologies were adapted by the smart card manufacturers as promising way to provide silicon fingerprints and creating cryptographic keys which are unique to individual smart cards. Following are the main advantages of smart card based CAS, especially in the context of interoperable STB.

Highly secure: With emergence of new technologies in smart card designs, they have become much more secure. There are numerous security measures being incorporated in smart card design nowadays to such as use of sensors to detect probing, fault injection by voltage glitch, laser light or EM flux, use of internal voltage regulators, internal clock sources, clock conditioning, symmetric design, dual rail logic, bus confusion, storage and transfer of data in encrypted form. Some manufacturers use PUF technology which is considered to be most secure against cloning attacks. Use of proprietary IC layouts, circuit designs makes reverse engineering attacks much more difficult. Apart from hardware, security threats are also mitigated by software measures such as software obfuscation, white box cryptography, etc. Also due to increased processing power and on board memory, more complex software algorithms can be used to make it even harder to hack the system.

Ease and Cost of replacement: Even after all security measures taken, newer security threats emerge out of technological advances as technology on field gets older. Broadcaster has to be ready for worst case scenario i.e. replacement of all field devices. Since in case of smart card based CAS, most of the security algorithms are placed inside smart card and there is very little dependency on STB, it is easier to replace all smart cards deployed by newer smart cards with newer security algorithms and countermeasures. On the other hand, in case of other types of CAS, all STBs have to be replace which is costly and difficult.

Ease of changing network operator: Smart card based CAS are easier to make interoperable wherein customer can use same STB for different network operators by just replacing the smart card of one operator with that of another. All the operator specific security schemes can be incorporated inside the smart card. In this way, Freedom for proprietary algorithms: Since operators can choose the smart card vendor and specifications themselves, they get the freedom of implementing any security scheme as they want by choosing smart card with specifications required for it. Also they can deploy different security schemes or completely different CAS at the same time in different service areas.

Portability: Due to its small form factor, smart cards are portable and user can carry it along anywhere he goes. So he can just put that smart card in the compatible STB and enjoy the channels he prefers to watch as long as he is in the service area covered by his operator. Also smart cards can store any user specific information such as programming reminders, parental control settings and many other preferences which can add to user's personalized experience.

Operational & Psychological Factor: In case of interoperability, when an user shifts to a new operator, if the new operator provides the user with a new physical entity (like new SIM as in case of Mobile) it provides operational advantages and also some sort of psychological comforts.

6. CA Message Filter:

The encoding and decoding logic of every CA message is left to the CAS but the CA message has to be inserted in the TS container in a standard way and each operator should follow the same for the given type of CA message.

The CA message filter in the interoperable STB is merely a TS packet filter for a particular CAS, the STB is configured using the SC. However, the CA filter shall be implemented using the following considerations based on ETR 289.

a) ECM shall use either 0x80 or 0x81 for the table id and the PID is as mentioned in the PMT as per standards.

b) EMM shall use the PID as mentioned in CAT and the Table id shall be in the range (0x82-0x8f) as defined in ETR 289. It is recommended to use the EMM structure as standard upto the User group ID field as mentioned the consultation paper to achieve interoperability.

c) The OTP trigger message shall also use the same PID chosen for EMM as provided in CAT but the table_id shall be used a fixed value which is same to all the operators. (Say 0x82 in the range 0x82-0x8f, but other than the table_id value used for EMM).

That way the CA Message filter for extracting/de-multiplexing CA messages shall be generic for any operator/CA.

7. Compatibility wrt different Modulation and Compression/encoding schemes:

Different modulation Schemes & Compression Standards being used are DVB-S, DVB-S2 & the new DVB-S2X and MPEG2, MPEG4 & H.265 Video Codecs MPEG2 / H.264 / H.265 Audio Codecs – MP2, AAC, AAC v2, Dolby.

Only backward compatibility can be ensured. MPEG4 is backward compatible to MPEG 2. MPEG2 audio is backward compatible to MPEG1. AC-3 is backward compatible with E-AC3. However, HEVC is not backward compatible with MPEG4/MPEG2. There are many royalty free audio /video codecs as well among the above mentioned list, so the royalty cost is not always involved. Going by the deployment today and the technology trend, a basic minimum set to be defined for STB. STBs can support additional codecs to have maximum coverages for different operators.

Different generations of STBs can be defined for Indian market considering these features and this can be an ongoing process. The STBs needs to be backward compatible and not the operator's stream. Also, it is very much pertinent to mention in this context that, these compatibility issues arising out of technology advancements relevant for every domains & verticals like mobile communication segments etc. The solution lies in structurally managing this rather than a very unstructured ad-hoc approach resulting in a very inefficient fractured, closed/rigid limited proliferation. This is ultimately not beneficial to the end consumer although it may appear to be serving the purpose in a very short term, when viewed in a skewed perspective.

SECTION II

C-DOT response/comments to the specific queries to the consultation paper dated 11th November 2019:

Q1. In view of the implications of non-interoperability, is it desirable to have interoperability of STBs? Please provide reasoning for your comment.

Comment: It is always desirable to have interoperability of STBs as already mentioned in various TRAI consultation papers. Major advantages are reduction in e-waste, freedom to the end consumers and industrial growth by opening up of the segment.

Q2. Looking at the similar structure of STB in cable and DTH segment, with difference only in the channel modulation and frequency range, would it be desirable to have universal interoperability i.e. same STB to be usable on both DTH or Cable platform? Or should there be a policy/ regulation to implement interoperability only within a platform, i.e. within the DTH network and within the Cable TV segment? Please provide your comment with detailed justifications.

Comment: Although technically feasible, this should not be attempted in the first phase as part of STB interoperability initiative due to cost implications of such a product. First phase of interoperability should focus on interoperability within Cable and DTH segments separately. That is, within individual segments of basic one-way distribution platform that constitutes the major percentage as on date. The major technical/rollout challenges will be addressed by piloting/introducing interoperability in one-way cable & DTH segment separately. Interoperability of STB across the cable & DTH segment is more of a product development challenge/task rather than a core technology problem to be addressed. If interoperability is taken forward within individual segments, the industry and market forces will probably enable much smoother adoption of interoperability across segments.

Q3. Should interoperable STBs be made available through open market only to exploit benefits of commoditization of the device? Please elaborate.

Comment: Yes

Q4. Do you think that introducing STB interoperability is absolutely necessary with a view to reduce environmental impact caused by e-waste generated by non-interoperability of STBs?

Comment: There are various ways of reducing e-waste including STB interoperability.

Q5. Is non-interoperability of STBs proving to be a hindrance in perfect competition in distribution of broadcasting services? Give your comments with justification.

Comment: Yes

Q6. How interoperability of STBs can be implemented in Indian markets in view of the discussion in Chapter III? Are there any software based solution(s) that can enable interoperability without compromising content security? If yes, please provide details.

Comment: At the outset, it is not very clear what is meant by software based solution. Any practical solution will invariably have some hardware and some software components built in it and shall work coherently to execute the desired functionalities. However, it is extremely relevant and contextual to mention here that, any solution that relies upon software programmable security is always an issue from core security point of view. As a practice, always the critical security components are physically realised through secure, tamper proof hardware, rather than pure software. That is practically the reason why OTP (One Time Programmable) memory fuses are used and programming/fusing of those are done either in the Silicon Fabrication time or through a very special tool. Any type of re-programmability, by definition, creates holes for security exploitation. This is more so in scenarios of one way networks. In a one way network, many well proven & promising security mechanisms based on "Challenge-Response" cryptographic schemes cannot be used (From STB there is no reverse channel to Headend in a traditional cable/DTH STB). Isolated secure software executing on a secure processor may augment the overall solution, but none the less, it is very clear that only software based solution (without specific hardware component) cannot be an answer to STB interoperability given the challenges of **one-way broadcast network** and other prevailing factors of the ecosystem.

Even in a highly open and reasonably standardized paradigm of software updates (and mostly security modules are not involved) in **two way connected** PC/tablets/mobile phones, where the update is from the same vendor/agency creates issues; given this practical reality, updating a secure module (only through remote software as being envisaged in some of the schemes for STB interoperability) where multiple stakeholders are involved, that too in **a one way network** seems to be practically too far.

Moreover, with high penetration of mobile phones in the country (India), the general public (more so with the people at the bottom of the pyramid) are comfortable (both psychologically & operationally) with the paradigm of SIM and mobile phones; going by these very important and pertinent facts, it will really be a much smoother roll out in India

when STB interoperability using Smart card is introduced. There are numerous studies done by researchers on various facets of high co-relation, interdependency that exists between psychological factors and information security. The concept of "useable security" suggests strongly that security method that is easy to use actually ends up being followed properly in operational scenarios and as a result, it actually ends up providing more security than an unconventional/difficult to use method.

Q7. Please comment on the timelines for the development of eco-system to deploy interoperable STBs for your recommended/ suggested solution.

Comment: For the approach based on ECI, availability of STB SoC complying with ETSI GS ECI specifications as on date to be ascertained. It is also to be noted that not only the availability of complied & certified (certification is extremely essential for interoperability) physical SoC is needed, but the whole SDK (Software Development Kit) around such SoC is essentially to be available & stabilised for usage of the SoC while designing the interoperable STB. After the tested SoCs are made available, the other components/modules of the value chain needs to be modified, integrated and tested in lab and in the field before the pilot trial begins. At this stage, this seems to be very far.

C-DOT has done the reference implementation of STB interoperability (based on Smart card based approach) as knowledge partner to TRAI, meeting/addressing all the security requirements (as mentioned in section I of this document) and same has been lab tested; prototypes are ready. All the interface details are prepared and some are already shared with the relevant stakeholders. One of the very important aspects of C-DOT solution architecture/approach is that it genuinely enables the industry stakeholders and provides them enough space for innovation in the product differentiation sphere. Also standardization process has been initiated by TEC (Telecom Engineering Centre, Govt of India) in consultation with C-DOT, TRAI and other stakeholders. Certificate generation part of TA (Trusted Authority) has already been done by C-DAC (Pune) in consultation with C-DOT as per details shared by C-DOT. The relevant stakeholders of the ecosystem can make use of the detail specifications and other relevant details to speedup the deployment of interoperable STB. C-DOT is ready for transfer of technology (ToT) for country wide adoption of the same. If needed, further fine tuning of the interface details etc. can be done in consultation with relevant stakeholders, as we proceed, based on deployment scenarios and feedbacks thereof. As already mentioned, better cost and space optimization of smart card/smart card connectors can be achieved by using smaller form factors such as SIM cards. Given the above factors, deployment (using C-DOT

solution architecture) can begin with quick completion of pilot trial involving interested stakeholders.

Q8. Do you agree that software-based solutions to provide interoperability of STBs would be more efficient, reduce cost of STB, adaptable and easy to implement than the hardware-based solutions? If so, do you agree ETSI GS ECI 001 (01-06) standards can be adopted as an option for STB interoperability? Give your comments with reasons and justifications.

Comment: The issues wrt software based solution are mentioned as part of comment to Q6 above.

Additionally following points to be noted:

1. Although at the outset, ETSI GS ECI standard seems to be apt for a two way STB, it is not clear about the applicability/feasibility/suitability of this standard for a one-way broadcast network. The challenges in a one-way network are very different than two way network such as IP networks. Hence before finalizing any approach for STB interoperability for a one way Broadcast network, the approach needs to be analysed deeply considering all the prevailing factors.

2. It is not clear how will the multiple CAS be supported? Does it require multiple root keys to be stored/pre-programed in OTP memory of SoC? Is the root key derivation/keyladder function similar to ETSI 103 162? Do the reasons for non-availability of a ETSI 103 162 (in totality) complied SoC/deployment framework has any implication on success of ECI based approach? These points need to be taken into consideration before thinking of adopting a standard that is yet to mature.

3. How will it support a new CAS entrant in the network?

4. It is not evident whether and how this approach takes care of hardware cloning which is becoming a major security challenge in today's networks. As content security technology and also hacking expertise move forward, there should be proper mechanism in place to take care of cloning issues in order to be future proof. Else, by the time the solutions are implemented, lab tested, field tested and deployed, it would become out dated and prone to security hacking and thereby not serving the main purpose & intent.

5. In the Indian context, where it is an extremely cost sensitive market, the additional requirements of memory foot print due to usage of multiple instances of virtual machines etc. (as per ETSI GS ECI), will surely increase the cost. It is pertinent to mention here that,

as on date, due to cost constrains (to reduce the memory foot print), many STB designers are hesitant to even go with open domain linux based solution (that is much less software intensive compared to the requirements mentioned in this standard); rather many of them opt for a lean proprietary/alternate smaller foot print OS. Hence this point needs a much deeper objective analysis.

6. VMs are used in ECI approach, VM (Virtual Machines) also have substantial threat vectors.

7. In ECI based approach, role and interfaces of TA is increased.

8. An additional new entity, Trusted Third Party (TPP) got added in the ECI based approach/framework. This makes the whole work flow very cumbersome and complicated, thereby giving enough scope for leakages.

9. This scheme will require changes not only in present day STB/SoC but in other modules of CAS/middleware/Headend as well, even for a two way network.

10. Availability of STB SoC complying with ETSI GS ECI specifications as on date to be seen. At the outset, it is evident that as on date there is no SoC complying with this standard. It is for sure that, there will be additional modules such as public key crypto engines etc. (along with other modules) needs to be augmented inside most of the present day SoC designs. After the tested SoCs with all the required additional features are made available, the other components/modules need to be modified, integrated and tested in lab and in the field before the pilot trial begins. It is often seen that there are many standards available with standardization bodies, but adoption of those takes time due to readiness of physical modules and inherent weakness/inappropriateness of some of these standards in the given deployment context/country specific ecosystem. It may not be out of context to mention that even after almost 10 years of release of the standard (ETSI 103 162), how many chipsets/deployment frameworks are fully compliant to this (in totality, except basic key ladder functionalities)? And the field adoption of this standard towards interoperability does not seem encouraging either.
11. Is there a reference implementation available as on date complying with this standard? In absence of this, it will always be a risky and time consuming proposition.

12. It is understood from the available documents that the standard is not complete in all aspects such as compliance, robustness rules, certification etc. In absence of such

important details, implementation and rollout of systems adhering to such standard will lead to a very chaotic situation and a futile exercise, especially where there are so many stakeholders in the value chain.

13. Apart from core technical and implementation issues, the operational aspects w.r.t interoperability using this approach are to be seen in correct perspectives in a vast and diverse country like India (unlike most of the European and other developed Countries). With high penetration of mobile phones in the country (India), the general public (more so with the people at the bottom of the pyramid) are comfortable (both psychologically & operationally) with the paradigm of SIM and mobile phones; going by this very important and pertinent fact, it will be a much smoother roll out in India when STB interoperability using Smart card is introduced.

14. C-DOT framework leverages on mobile penetration in the country to enhance the level of security.

15. India is a vast country with more than 130 crore population, it is indeed more prudent to go for a standard more relevant and suitable to our country (India), like some of the initiatives taken in countries like China having their own country specific standards and solutions in many technology verticals including this vertical; rather than trying for a standard developed in a totally different ecosystem perhaps.

Q9. Given that most of the STB interoperability solutions become feasible through a common agency defined as Trusted Authority, please suggest the structure of the Trusted Authority. Should the trusted authority be an Industry led body or a statutory agency to carry out the mandate? Provide detailed comments/ suggestion on the certification procedure?

Comment: No comments at this stage.

Q10. What precaution should be taken at planning stage to smoothly adopt solution for interoperability of STBs in Indian market? Do you envisage a need for trial run/pilot deployment? If so, kindly provide detailed comments.

Comment: The approach for STB interoperability is to be driven by India's context and requirements. So far as possible, the approach and the solution shall be such that it does encourage value addition, IP (intellectual Property) creation, industrial growth inside the country along with primary objectives of consumer freedom/benefits in the true sense

and in a sustainable way, with maximum self-reliance. Extra precautions to be taken to avoid external dependencies and direct / indirect vendor locking through a holistic assessment of the problem, solution and ecosystem.

After lab testing, Pilot trial is indeed necessary for STB interoperability. Only interested & serious stakeholders need to get involved in the pilot trial. Proper MoU (Memorandum of Understanding) needs to be signed between all the stakeholders with both penalty and incentive clauses for the purpose of pilot trial with the scope well defined for each stakeholder. The case where a reference implementation is already lab tested and scope for all the stakeholders gets well formalized, the pilot trial can be executed without much of a hassle.

Q11. Interoperability is expected to commoditize STBs. Do you agree that introducing white label STB will create more competitions and enhance service offerings from operator? As such, in your opinion what cost reductions do you foresee by implementation of interoperability of STBs?

Comment: A carefully selected approach will definitely help in cost reduction after sometime.

Q.12 Is there any way by which interoperability of set-top box can be implemented for existing set top boxes also? Give your suggestions with justification including technical and commercial methodology?

Comment: Practically seems infeasible.

Q13. Any other issues which you may like to raise related to interoperability of STBs

Comment: A lab tested and indigenous solution will surely be more prudent for immediate pilot run followed by rollout, rather than untested, yet to mature approaches. It is important that few execution aspects to be streamlined, formalised and taken care by the relevant stakeholders for timely completion of Pilot Trial. C-DOT solution that is very apt for one way broadcast network, can be tweaked, adapted and augmented little bit more to cater to OTT STB segments (in a two way network) as well with a cardless variant. C-DOT has been working in that direction also, keeping in perspective India's context and technological advancement in enabling technologies, in a coherent manner. One of the very important aspects of C-DOT solution architecture/approach is that it enables & equips the industry stakeholders and provides them ample space for innovation in the product differentiation sphere. IP (Intellectual Property) creation, value

addition/creation and manufacturing boost in the country needs to be encouraged to meet the end customer benefits in a sustainable manner and there by becoming a true enabler to flagship programmes of Government of India such as “Make in India” (by indigenous design & manufacturing of STB) , “Digital India”, “Skill India” (Repair & service centres across the country for STB) and “Start Up India” (Third party applications development by startups). C-DOT reiterates its commitments to these flagship programmes and hopeful to play a more pivotal role in that direction along with TRAI and other stakeholders in future.