28th August, 2017

To,

Mr. S.K. Singhal
Advisor (B&CS)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi-110 002

Ref:- Consultation Note on Solution Architecture for Technical Interoperable Set Top Box dated 11th August, 2017

Dear Sir,

At the outset, we would like to put on record our sincere appreciation for all endeavors and measures which the Hon. Authority has been taking in the recent past, to systematically regularize the sector by periodically introducing diverse regulations and deeply involving the stakeholders in its processes.

So far as the above captioned Consultation Note is concerned, we would like to reiterate our consistent stand in respect of Technical Interoperability of Set Top Boxes, taken by us in our various previous comments to similar consultation processes on the subject.

Before we deal with all historical development in the endeavors of the Hon. Authority to introduce of Technical Interoperability in the DTH industry in detail, we would like to summarize the technical and all other limitations for the current endeavor under the Consultation Note, as given in the Summary of Responses for C-DOT framework of STB Interoperability annexed hereto as **Annexure A**.

Historical background:-

As the Authority is aware the exercise of introduction and implementation of technical interoperability in the DTH industry has remained at the realm of deliberations with stakeholders since 2006 and continues to remain so till the authority coming out with the

present Consultation Note on Solution Architecture for Technical Interoperable Set Top Box dated 11th August, 2017.

Despite the Hon. Authority making specific recommendations relating to interoperability on January 30, 2008, the situation has remained the same even today. It is pertinent to note that the Ministry of Information and Broadcasting had specifically commented about the concept of Technical Interoperability as being costly, anti-consumer, impracticable, unfeasible, and on various other grounds had requested the authority to re-visit and re-examine all issues related to Technical Interoperability.

Since the Ministry of Information and Broadcasting had returned the recommendations of the Authority dated 30th January, 2008, a fresh consultation paper on Technical Interoperability of Set Top Boxes was released by the Hon. Authority on 20th August, 2010. Whilst responding to queries under the said Consultation Paper, practically all stakeholders had strongly advocated the idea of relinquishing the introduction and implementation of Technical Interoperability, on grounds ranging from expensive CAM module, questionable cost-effectiveness and anti-consumer elements and also achievement of fully successful commercial interoperability. As the Authority is aware, this was the last Consultation Paper purely for Technical Interoperability and pursuant to which no recommendations were made.

We would like to emphasis on the fact that despite the long duration exercise of Consultation Paper of 2010, nothing concrete has emerged out of it. In fact, we are besieged in the midst of absolute confusion emanating from multiple exercises on implementation of Commercial Interoperability and our endeavors of introduction of Technical Interoperability, with roles of a DTH service providers and customers as to security deposit, refund, surrender of CPE, use of refurbished STBs, CPEs, getting converse or reverse in the two systems of Interoperability.

It will not be out of place to mention here that till the release of the current Consultation Note on Solution Architecture for Technical Interoperable Set Top Box, the consultation paper of 20th August, 2010 was the last endeavor on introduction of Technical Interoperability, with the feasibility and practicability of the same remaining always under doubt and question.

As the Authority is further aware that on 23rd July, 2014, Recommendations on Issues Related to New DTH Licenses were released by the Authority. In these recommendations the Hon. Authority recommended on the issue of Interoperability of DTH STBs as follows:

i. ***The license condition prescribed at clause 7.1 of the existing DTH Guidelines should be replaced with the following clause:***
"The Set Top Box offered by a DTH service provider shall have such specifications as laid down by the BIS from time to time."

ii. ***BIS should come out with updated specifications for STBs from time to time and while doing so, BIS shall consult TRAI.***

iii. ***The license conditions should mandate the licensee to comply with the tariff order/scheme prescribed by TRAI for commercial interoperability.***

These recommendations were once again reiterated in the Authority's Report on Activities between 1st January 2014 and 31st December 2014. As the Authority is aware the above recommendations are still pending for consideration with the Ministry and as such stakeholders have no clarity about the probable outcome of these recommendations.

However, before the Ministry of Information and Broadcasting responded on the aforesaid recommendations of the Hon. Authority, another Pre-consultation paper on Set Top Box Interoperability was released on 4th April, 2016. Practically all stakeholders once again objected to the introduction and implementation of the concept of the Technical Interoperability on various grounds mentioned in their respective responses, therein elaborating those grounds in a logical manner. We would urge the Hon. Authority to kindly relook and re-examine the grounds of opposition raised by the stakeholders in their respective comments, which is part of the record.

The Authority is well aware of the Order passed by TDSAT in the matter of CA 9035 /2011 Tamil Nadu Progressive Consumer Centre vs. Ministry of Information and Broadcasting; in which BIS has been advised to work in sync with TRAI, in order to ensure that appropriate applicable standards are achieved within a stipulated time period in the said Order. However, all Stakeholders are grappling in the dark about any sort of development in this respect as well.

TRAI is further aware that Tamil Nadu Progressive Consumer Centre has filed appeal against the order of TDSAT and the same is pending before the Hon'ble Supreme Court and as such the entire gamut of Technical Interoperability is sub judice and hence the current exercise cannot be proceeded with any further.

Moreover when commercial interoperability has been admittedly achieved thereby is facilitating the consumer to shift form one operator to the other easily. Issue of Technical Interoperability has subsided altogether. It will not be out of place to mention that even in coming out with new QOS regulation dated 03rd March, 2017, the Authority has authorized the customers to swap operators by returning the STB and ODU to the earlier operator.

Conclusion

Since the current Consultation Note on Solution Architecture for Technical Interoperable Set Top Box has been released pursuant to the Pre-consultation Paper on Set Top Box Interoperability, it is all the more important for the Hon. Authority to ensure that ALL concerns of not only stakeholders are redressed to the hilt but also be assured of a consumer friendly environment for all subscribers now or in future. In case only partial solution is achieved in redressing the concerns of the stakeholders pursuant to the current Consultation Note, then it would not be prudent to go ahead with the exercise at all. In this regard we would once again reiterate what has been stated by us in our response to the Pre-consultation Paper on Set Top Box Interoperability was released on 4th April, 2016 and would request the authority to read the same in the context of the present Consultation Note.

Considering all unresolved and unanswered questions surrounding the Technical Interoperability, we would beseech the Hon' Authority to allow commercial interoperability to sustain and drop the current exercise of the suggested model under the present Consultation Note.

Annexure A

Replies for C-DOT Framework and Feature Requirements

The key primary weakness in the proposed system is on the SoC / decoder Chipset side

1. In the recent years, we have seen hackers mainly focus their efforts on attacking the SoC (System on Chip- STB chipset)
2. Poor security implementation of standards in SOCs may lead to STBs hacked across Service Providers on the proposed interoperable STBs.
3. A proprietary HW block in SOC doesn't solely depend on obscurity, rigorous testing through design & implementation & QA by CA vendor provides a much higher level of security than only a standards based solution.
4. A proprietary HW block provides a very high level of security, one that could be used alone without smartcards and help reduce cost.
5. Also in today's world, security is not only depending on the robustness of CAS, EMM and ECM but also SoC security blocks, Key Ladder, Boot loader, Memory, TEE of SoC. Hence if STB is not secured, piracy cannot be prevented or blocked. The need for reduced-price STBs has besides security being a main driver towards card less CAS designs, as smart cards and associated logistics are a major cost driver in the design and maintenance of the STB. A multi-operator STB would also for user convenience have several card slots also driving cost.

Control Word protection logic must reside in HW

1. STB software can almost always be compromised
2. The current proposal indicates that significant portions of the key material would reside in STB RAM at some point, exposing the system to significant hacking options
3. The dependence on asymmetric cryptography and certificates on the critical path of this SW scheme is particularly major worrisome
4. Private key management are susceptible to side channel attacks. If even one private key is leaked, the system is essentially broken

Root of Trust is key aspect and it is not considered

1. The existing proposal by C-Dot has been lacking in not understanding the current threats and the security environment in STB.

2. Current proposed new centrally controlled and monitored key mechanism is highly vulnerable and this security lapse may adversely impact the entire pay TV system of the country in case of any security threats and hacks.
3. The entire content protection can be hacked when the hackers get an access to the "Control Word" and its propagation over the internet, so that it can be input separately without the smartcard.
4. The other feasible option is to have card less CAS set-top boxes, equipped with a hardware-based root-of-trust.
   A hardware root-of-trust, provided by many platforms offers operators robust security protection with an integrated security core (SoC) which cannot be tampered and the "Control Word" is not under communication outside the security core protected main SoC.

STB Cost also be a key factor

1. The need for low cost STBs has led to card less CAS designs, as smart cards are a major cost driver in the design and maintenance of the STB. A solution as proposed by C-DoT is highly risky as the smartcard based solution leaves the decryption open to "side channel attacks".
2. Current communication between the Smartcard and the STB are secured is itself prone to attacks and can be easily compromised in the absence of a separate root of trust.
3. Thus, instead of the on-going developments in the field being of interest to the customers, whereby the cost of the STB can fall to below $10-12 in a year's time, the situation will reverse and customers will need to pay more for a proposed C-DOT solution.
4. Moreover, with the current low cost of STBs, the migration of customers has become trivial as the cost of the STB is a marginal component of the total cost over a 3-year period I.e. $3-4 per year.

Lifecycle Management

1. Every Private keys must be secured not just while in use, but throughout their entire life-cycle

2. STB manufacturers have not been responsible for safeguarding these system-level secrets and it is unclear that they have the facilities, knowledge and experience required to design and implement such systems.

Countermeasures Limitations

In a well-designed system, counter-measures are implemented by CA HW modules (SoC and/or smart-card) and are used against various attacks on a service provider.

The proposed architecture limits counter-measures that can be used:

The inclusion of devices that do not support these counter-measures prevents the CA providers from deploying their most effective weapons in the fight against piracy.

Some of the counter-measures detect differences between the legal devices and illegal ones.

Having a global, standardized and publicly known requirements for the STB functionality will make it easier for the attacker to implement a similar functionality in an illegal device, or hack the legal device in order to attack the system – in both cases, most of the countermeasures will fail to identify the illegitimate usage.

Major Impact to Existing operational Systems

Proposed system will significantly impact functionality of existing multiple levels

1. Change to Card/STB CA SW (Verifier) API: will impacts both Headend and Client system components
2. STB-Card-Mobile # coupling in the CA system for every subscriber: impacts the control plane and back office services, including the 3rd-party Subscribers Management System
3. New EMM structure to support portioning to Group IDs: in addition to the impact on the CA components (HE, Client and Smartcard) this could result with an impact on the EMM bandwidth
4. Maintenance & delivery of CA certificates for smartcard and STB: significant operational impact.

Standardized MW implications

1. For a 3rd party to develop middleware, there also needs to be a standardized hardware and software environment specified. Such specification in other countries, has significantly increased the cost of hardware.
2. This implies there is a need for per operator certification and testing of each of the middleware software, against each hardware type, which is a significant time consuming and expensive exercise.
3. Advanced middleware functionalities such as PVR would need further development of specifications to ensure proper content security and rights handling.
4. If multiple manufacturer enabled middleware are to used, then based on each implementation and platform's capability and performance, there can be a very inconsistent user experience that can lead to consumer frustration.

EPG Implications

1. Simple EPGs proposed, which are not operator specific need an agreement on the extent of features supported such as finger- printing, OPPV, broadcast mail/messaging. This needs a detailed EPG spec defined.
2. Advanced EPGs which can be operator specific, would require an advanced middleware specification similar to MHP/OCAP. The experience in MHP and OCAP have proved that even applications developed against these specifications require hardware specific integration and long validation cycles. This is because the performance/stability can be highly dependent on the specific hardware and platform driver capability

Software Upgrade Implications

1. If any STB sold in India must work under any operator then the operators will have to support the ability to carry the upgrade images of ALL and ANY new such devices manufactured for India.
2. The maintenance and management of new images due to new features added or bug fixes found against each platform can be extremely challenging and expensive.

Operator Services and Signaling

1. The system proposes to use standard DVB signaling of services and metadata.
2. The Indian satellite eco system has grown with specific needs which require extensions to DVB for offering acceptable end customer experience w.r.t. discovering content as well ability to support multiple languages in a scalable way.
3. An additional comprehensive new specification is to support the current content discovery experience.

Key summary points

1. Current proposed implementations has many security concerns and it is not a foolproof mechanism to adopt
2. HW cost would be heavy to incorporate the changes
3. Common standard approach will make the hackers to attack the box easily and any illegitimate thing can be done easily
4. Proposed implementation heavily impacts both Headend and Client system components which would involve high commercial for an DTH service provider
5. Common standard will impacts the major changes in existing operational works and back office services, resulting in unnecessary heavy bandwidth consumption

6. Having one common STB with set specifications will kill innovation