INDUSIND MEDIA & COMMUNICATIONS LIMITED

Date:25/8/2017

To,
Mr. S.K.Singhal
Advisor
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
New Delhi-110002.

Subject: Comments on Consultation Note on Solution Architecture for Technical Interoperable Set Top Box, dated Aug 11 , 2017

Dear Sirs,
We thank you for giving us the opportunity to respond to the consultation note on the Solution Architecture for Technical Interoperable Set Top Box. As DPOs, our business is not buying and selling of STBs , but rather the delivery of video services to our customers. The capability for customers to purchase STBs individually significantly reduces our burden in terms of maintaining stock and large quantities of assets on our books. Also, financially, the impact on DPOs will be substantial as the investment required to support the issuing of STBs no longer lies with us nor is there any burden on DPOs to subsidise the hardware for customers. The most immediate impact from the customer perspective will be that they will now need to bear the entire cost of the hardware upfront themselves, which in most cases (particularly in cable & HITS) has been heavily subsidised during the DAS rollout.
Whilst we agree with the premise that customer service should always be at the forefront of all service providers under the direction of the associated Regulatory body (TRAI), the current solution proposed for the Technical Interoperable STB does not meet all the requirements or framework proposed by TRAI, particularly in relation to security and the capability for DPOs to offer more enhanced services in their STBs. We believe that commercial interoperability would be more efficient in delivering the customer satisfaction that TRAI is looking to enhance, at least until a workable technical interoperability has been developed and tested on the ground.

We have herewith enclosed our comments on the consultation paper questions.

Yours sincerely,

(Ashok Mansukhani)
MD & CEO, IndusInd Media & Communications Limited (MSO)
MD & CEO, Grant Investrade Limited (HITS)

Our response is divided into the following sections:

1. Framework for interoperable STBs as proposed by TRAI
2. Operational impacts envisaged when implementing the proposed technical solution architecture
3. Conclusions

Framework for Interoperable STBs

The Telecom Regulatory Authority of India (TRAI) has, *suomotu*, taken up the issue of technical interoperability of STBs. The framework of interoperable STBs proposed must ensure the following as per the Consultation Note:

1. The level of security should be similar to or better that what is present today.
2. The framework must be sound enough to prevent reception of services by unauthorised persons
3. The prices of the interoperable STBs should remain comparable to non-interoperable STBs
4. The portability cost should reduce considerably
5. The DPOs should be able to choose security solutions (Conditional Access System) as per their requirements
6. The proposed solution must be able to identify pirates, if any
7. The UI and EPG format customisation
8. The framework should ensure that TV channels with EPG listing continue to be available to the consumers on migration to another operator

The technical solution architecture proposed in the consultation note in our opinion does not meet all the framework requirements above for the following reasons:

1. **"The level of security should be similar to or better that what is present today."** The level of security of the proposed architecture is not as strong as what is currently available today:
    a. The STB manufacturer is now responsible for the secure bootloader. Previously this would be certified by the CAS vendor but now this additional security check is eliminated.
    b. The chipset's software will have access to the unencrypted control word within the chipset. This is not best practice from a security perspective and could be easily hacked.
    c. The STB manufacturer is now responsible for the STB software. If this has not been written correctly or securely, then there are more chances of piracy/hacking taking place. There must be an entity set up who can certify that the software developed by STB manufacturers is secure.
    d. It is not clear in the solution architecture document who will be responsible for certifying each STB model as being secure and therefore who takes responsibility for the same. In the event an unscrupulous STB manufacturer does not follow all the

security requirements, then the STB and all DPO services could be subjected to hacking.

e. Responsibility for content security in the hardware device is now further fragmented than before. More responsibility is now being placed on security on the part of the STB manufacturer which was not there before or at least controlled and certified by the CAS vendor. Without a certifying body, the security of the STB hardware could seriously be hampered. Also, most STB manufacturers are not within the country and their management will become even more difficult.

f. The HITS service provided by Grant Investrade Limited also has additional security in-built into the STB software to protect STBs from moving from one headend to the other. In order for this security to be maintained, it would have to be replicated by every STB manufacturer in their own software. The distribution of this security design to all STB manufacturers would compromise the security of the HITS service, even if this was covered by non-disclosure agreements. Alternatively, HITS would have to remove this security layer which would again further compromise its security enabling any cable operator outside of the Indian border to also receive the signals of the HITS service.

2. **"The framework must be sound enough to prevent reception of services by unauthorised persons".** The capability to handle content piracy becomes more difficult for broadcasters and DPOs. Typically, a broadcaster handles cases of content piracy by sending its own fingerprint and requesting the same of the DPO who is using their IRD. This enables the DPO and broadcaster to uniquely identify the STB in question and shutdown the smartcard associated with the piracy. In the case of fully interoperable STBs, this capability could be severely hampered. In the event a pirate sees fingerprints coming on the STB that are "outside" of normal circumstances, then the pirates could easily switch over to a new smartcard from a different or same operator, thereby making the process of switching off a pirated signal much more difficult for broadcasters.

   According to the CAS vendors, the proposed solution design also adds further points where security could be compromised within the STB itself, including increasing the chances of smartcard sharing, exposure of the control words etc. The solution must be able to satisfy CAS vendors that the existing security points will not be further impacted.

3. **"The prices of the interoperable STBs should remain comparable to non-interoperable STBs".** The requirement to support the technical interoperability will inevitably increase the costs of the STBs for the following reasons:

   a. CAS vendors will have to develop new smart card technologies to support this new architecture. This cost will inevitably be passed on to the customers indirectly by the DPOs.

   b. All STBs certified will need to be certified by all the CAS vendors which will again add further cost. Currently certification is done only for those STBs that a DPO requires.

c. DPOs will need to have the STB manufacturers develop versions of software for each of their STB models. Again, this will take time and add additional cost to the STB which will, inevitably, be passed on to the consumer

d. STBs will now be sold in the retail network for which retailers/distributors will also expect to receive a margin. Currently whilst the DPOs are purchasing the STBs themselves and in most cases also subsiding these, the cost to the consumer is very low. In the retail market, the cost of the STB will expect to increase at least 20% just to cover retail and distributor margins for stocking and selling these.

e. Retailers/manufacturers will also need to put in place their own service centres across the country to handle repairs and maintenance which are no longer the responsibility of the DPOs. This will also add further cost to the STB which could in part be offset through AMC models.

f. The proposed solution architecture is based on smart cards. Currently most CAS vendors have been moving to cardless or software-based CAS mechanisms to reduce the cost of the STBs and CAS for DPOs. Existing smart-cards would typically cost an operator USD3-7 whereas software or cardless CAS licenses have been reduced to USD1-3. This has significant cost impact on the DPO who needs to then purchase the smartcards. The new smartcards that will need to be designed to support the proposed solution architecture may be even more expensive depending on how much memory they require in order to store the additional data.

g. The chipsets in use today have been designed for specific types of STB functionality, including low-cost zapper STB solutions and corresponding price points. The proposed solution architecture will probably require additional processing power in the chipset in order to achieve the bi-directional authentication, EMM filtering etc. This will have the potential to add further cost to the STBs.

h. The patent for this solution architecture is owned by C-DOT. As such, C-DOT will need to confirm whether royalties/license fees will be applicable to STB manufacturers, DPOs and CAS vendors in order to use this solution architecture. This again could result in an increase of costs of the STBs for consumers.

i. DPOs will need to continuously stream versions of software for each STB model on the network in order to support "upgrading" the STB to the new DPOs software. This will significantly increase the bandwidth requirements for DTH/HITS players depending on the number of STBs being certified and needing to be supported.

There is nothing in the solution architecture that would indicate that the cost of the interoperable STBs would be cheaper than non-interoperable STBs. Infact, due to the additional processing power requirements and the move to card-based CAS (when many operators have instead moved to cheaper software/cardless based CAS systems) the cost of STBs are likely to increase to the consumer.
Further most STBs are subsidised to the end-consumer by the DPOs. When purchasing from the retail network, the subsidy will no longer be available to consumers.

4. **"The portability cost should reduce considerably".** The solution architecture will reduce the

immediate cost to customers to move from one DPO to another. However, there are other impacts:

a. Most STBs issued as part of DAS as well were heavily subsidised, sometimes more than 50%, for customers. Therefore, the cost to consumers was never the full value of the STB. When purchasing STBs from the retail market, consumers will be obliged to pay the full cost of the STB. There will be little inclination for DPOs to offer STBs in subsidised fashion as these can be easily migrated to other networks. This is particularly the case for MSOs where their linked LCOs could now easily move to another MSO very easily simply by swapping the smartcards.

b. Portability will be simpler for customers, but under the solution architecture proposed, this only applies to simple zapper STBs. The capability for STBs to offer enhanced and interactive services, including simple PVR (personal video recording) capabilities are not offered by this solution.

5. **"The proposed solution must be able to identify pirates, if any".** The proposed introduces additional places where pirates and hackers could affect the security of the encryption system, including in the STB software itself. Whilst the solution itself uses the same CAS encryption technologies already in place, it opens up the possibility for hackers to quickly switch service providers in the event that piracy is identified. The solution has to provide a solution for which STBs can be blacklisted so that they cannot work with any other provider and can be shutdown centrally by any CAS system in order to reduce piracy issues on the ground.

   CAS vendors have also raised concerns about the reduction in the security of the video signals in this architecture which will need to be addressed. In the event of a piracy/hacking breach, there is no clarity on who will be responsible for the breach.

Further there are other aspects that the framework does not cover that are as equally important both for consumers as well as DPOs:

1. **"STBs should be able to support today's current functionality or better."** The proposed solution architecture only supports basic zapper STBs with EPG functionality. There is no specification proposed for how other "basic" functionality that are available to many STBs already rolled out in the networks can be provided using this architecture:

   a. **PVR capabilities**- Many cable/DTH STBs today are being offered with USB-based PVR capabilities as standard that enable customers to record their content on any external hard disk device in encrypted format and play it only on the authorised STB. The technical solution architecture proposed does not identify how this functionality will be delivered by interoperable STBs. In most cases, the recorded video is stored in encrypted format using the CAS technology of the DPO and also includes the ECM data associated with that transmission in order to ensure that customers who no longer have the necessary rights for that channel can no longer view that content.

When a customer moves from one operator to another, the customer will lose the capability to view any of the previously recorded content.

b. **DPO security requirements** – The HITS service has developed specialised additional security into the STBs to ensure that movement of STBs between different DAS areas and locations is controlled. This is critical in ensuring that reporting for broadcasters is accurate and that piracy (e.g. moving of boxes across borders and DAS regions) is restricted. This security is not in-built into the CAS system and

c. **Interactive services / Games** – many of today's DPOs offer additional services on their STBs (e.g. games, interactive services etc.). There is no specification in the consultation note about how these can be achieved. These services are today available even on basic zapper STBs of these DPOs and are used by DPOs as additional revenue sources. The technical solution architecture must be able to address how additional operator-specific functionality can be developed and added into the STB software to enable customers to take advantage of these. Typically this functionality is built into the middleware, but there is no specification in the technical solution architecture as to how any middleware can be implemented on these STBs.

2. **"STBs should follow specific technical parameters" –** The solution architecture also does not specify the formats and technologies to be supported by these interoperable STBs. In the Indian scenario today, there are operators supporting MPEG2, MPEG4, HEVC encoding. In order for technical interoperability to work, then it will be important to specify the technology to be used. In the event that MPEG4 is selected as the standard encoding, then DPOs already offering HEVC content will not be able to meet technical interoperability. Customers will also need to know that they must purchase this minimum specification in order to connect to that DPO's specific network.

The framework also only covers "technical" aspects, but does not put a framework towards how it will improve or impact operational issues in servicing and supporting customers.

Operational Impacts

The proposed solution architecture has various operational impacts that need to be considered in a final solution:

1. **QoS Regulation impacts** – as per the QoS regulations, DPOs must provide customers with options for leasing STBs as well as replacement of STBs within defined timelines. If DPOs are no longer responsible for the provision of STBs, then these QoS regulations will need to be amended accordingly. DPOs will not offer STBs to their customers directly, but rather request customers to purchase these directly from the retail market. The subsidy on STBs will also not be viable as there is no commitment from customers to stay with the service for any period.

2. **STB replacement and maintenance** – if customers have purchased their own STB, then DPOs cannot take responsibility for their repair or even the 12-month warranty mandated by the QoS regulations. The responsibility must now lie with the STB manufacturer or distributor/retailers who are selling the devices to the consumer. They will be required to maintain necessary service centres/repair centres in order to fix STBs who have failed.

   Retailer/distributor warranties typically relate to manufacturing failures. Whereas, DPOs have, up to now, been giving replacement boxes within 12 months even for customer-created failures (e.g. faulty electrics etc. that can cause reverse current or surges to destroy the STB) as a sign of goodwill and in the spirit of good customer service.

   The responsibility for providing 24-hour replacement cycle as mandated in the QoS draft regulations will no longer vest with the DPO as the ownership of the STB is no longer with the DPO. The customer will need to wait until the retailers/distributors' service centre can repair the STBs. During the repair period, customers may require to be able to "pause" their active packages in order to avoid paying for services whilst the STB is being repaired.

3. **Certification of new STB models& differentiation** – if a DPO wants to launch a new STB that is different from those already in the market, then it will need to approach which authorities to confirm the technical specifications? Also, this new STB model will need to be certified by all CAS vendors and software developed for all DPOs before it can be launched. This will add a large amount of deployment time for each STB model. Also, the capability for DPOs to launch STBs that differentiate their offerings from other DPOs will no longer be possible. The proposed model does not permit any differentiation of STB models between operators.

4. **OTP Mechanism** – the need to have customers send an OTP every 15-30days will be onerous on consumers. This facility should be extended beyond 30 days to make it customer friendly.

5. **Migration between Cable (DVB-C) and DTH (DVB-S/S2)** – there is no explanation in the solution architecture as to how customers can use their STB in both DVB-C and DVB-S/S2 modes. If the STBs must support both, then the solution will necessitate more costly tuners which will inevitably increase the cost of the STB. Also, if customers migrate from cable to DTH, or even from DTH to DTH, who will be responsible for moving dishes, providing dishes/LNB/Cables/Connectors etc. to the customer? Again, these are currently subsidised, but in the future DPOs will be forced to remove the subsidy if they have no guarantee that the customer will stay with them for any extended period.

6. **Prepaid vs postpaid** – the only way for DPOs to ensure revenue collections when STBs are technically interoperable is to move to fully pre-paid models from subscribers. This ensures that DPOs are able to collect their revenues upfront and that customers do not switch operator before payments take place as in post-paid mode.

Conclusion

Further clarification is required from TRAI and C-DOT on the areas of concern indicated above. Further it is suggested that CAS vendors who are currently responsible for video security also be involved more deeply in the discussions around technical interoperability in order to ensure that current security is not compromised or impacted. CAS vendors who have been specialising in video protection will also have knowledge of best practices in ensuring content security within the STB.

Grant Investrade Limited (HITS) and IndusInd Media & Communications Limited (MSO) would be keen to get involved in the development of PoC for interoperable STBs in conjunction with TRAI and C-DOT in order to try and deliver a workable platform that could deliver technical interoperability as envisaged by TRAI.

******

C-DOT Framework For Interoperable STB& Feature Requirements For Stakeholders Of The Ecosystem

V1.2

CAS :-

1) Today the CAS vendor takes liabilities for the Operator for protecting their content.

   As per the proposed framework; the TA, STB manufacturer and the operator are the custodians for the keys to implement the security.

   a. **Please clarify who will take the commercial liabilities in cases of piracy?**
   b. **Please also clarify what types of counter measures are available in this architecture?**

2) Since the framework is based upon the patents in the name of C-DoT (C-DOT patent: US8978057B2), will there be any royalty to be paid by a licensee for the use of the patent?

This is an important consideration to under the commercial viability keeping in mind that the objective is to reduce costs to the end-subscriber.

3) Will the patent holder provide a license to any company in India or outside of India?

4) Will there be any restrictions on number of STB manufacturers to operate under the interoperability framework?

5) In the proposed interoperable framework, any STB can access any Smart card (SC).

   This will increase the risk of the first level of hack, i.e. Card sharing.

Pirates can use a splitter (A splitter or ECM concentrator is a pirate device which allows a smart card to be shared amongst several STBs) to share SCs between several STBs. Using wireless splitters, it allows the sharing of subscription in the near neighbourhood or can be shared over internet.

It has been suggested in the framework document that the end user will have to send a SMS from his/her registered mobile number to the operator portal for renewal at a frequency which is yet to be decided in order to authenticate the correct pairing of the STB and SC.

Such an approach is not user friendly and may also result in loss of revenue till such time that the renewal process is complete.

It is recommended to use pairing using key ladders with properly defining the architecture.

6) Page-8, Section 5.1

Operator specific part of CAS in the smart card [ECM, EMM decryption etc.] retained unaltered leaving enough space for innovation by the CAS vendors.

Question :- As per the above point, ECM and EMM will be unaltered and it can remain same as the CAS operators structure but in the section – e and section 6.b #III C-DOT is proposing the EMM message structure.

So, is it mandatory to use the proposed format by C-DoT or the CAS vendor can implement its own format?

7) Page -27, Section 5.4 #b, XII and XV - Pairing-id

Question :-As STB and SC are provided with different keys, it is not clear on the process to generate the pairing id which has to match pairing id of STB and SC for authentication ?

If STB and SC generate different pairing ids then it will not match and the requirement mentioned in the point XV will not be executed. This will lead to the registration process failure.

Please let us know how STB and SC generates the unique and matching pairing id during the registration process in the interoperability scenario.

8) Page -26, Section 5.4 #b, X, - Control Filters

Question :-What information will be contained by the control filters in the Trigger message?

9) Page -25, Section 5.4 #b, V and VI, - Trigger Control Message

Question :-How will this Trigger control message sent to STB as this trigger control message is not ECM and EMM?

10) Page -27, Section 5.4 #b – OTP Process for Renewal

Suggestion :-All the CAS already have the feature of positive addressing which means it will not allow the user to watch the content if the subscription is not renewed.

Using this feature, we can avoid the periodically registration renewal process and hence improve user experience.

11) Page-29, Section 5.4 #d

Smart card decrypts EMM/ECM and private data (if present) to get CW and sent to de-scrambler in STB to de-scramble the audio/video signals.

It has been proposed to have the CW deciphered in the SoC and handled by the descrambler internally. It has also been proposed to use the session key to do so, but in order to keep the session key secret in the SoC, the whole session scheme has to be implemented in the SoC, which presents several difficulties for the SoC vendors:

- It means implementing RSA2048 which is gate consuming, especially if it has to be secured against side channel attacks.
- Implementing the AES block in the SoC is complex.
- As far as we are aware, no chipset currently available in the market has such a feature, hence it will be long before the first SoCs become commercially available.
- Such a specific feature will make the SoC more expensive for the Indian market, which goes against the initial goal.

The existing implementation of CW protection from SC to SoC involves the usage of key ladders, either proprietary or standard. Hence, it is suggestedto use a key ladder to enforce protection of CWs to the SoC.

12) Page-31, Section 5.4 #e

SC decodes only the EMMs meant for that subscriber.

Question :-This will increase the usage of CPU power for the STB as well as for the SC thus increasing the costs. This will also lead to processing of other metadata, zapping time to filter the correct ECM/EMM and may result in overall performance issues.

Suggestion:- There should be generic CA (Conditional Access) library inside the STB. This will help to discard the pre-processed EMMs which are in the carousel for a pre-defined time.

The CA Lib also helps to display the diagnostic information on the STB screen for the troubleshooting purpose.

13) Page-31, Section 5.4 #e - The GN and IK are kept totally uncorrelated.

Question :- Please clarify the role of IK.

14) Question : There is no mention in the proposed framework about how to prevent CW sharing in case the SoC gets hacked? Please advise.

15) Question: There is no mechanism proposed in the framework to prevent unauthorised leakage of keys by STB manufacturers.

16) Question: Majority of the deployed STB are using a cardless CAS instead of a SC due to the inherent cost advantages. With the proposed framework based on a SC architecture, it will increase the costs for operators and end-users.

Operations related :-

17) Currently in case of faulty STB, operator replaces with another STB. What will be the workflow for the STB maintenance?

18) Page-12, Section 5.2

The digital set top box receives the MPEG-2 TS through RF tuner, demodulator & decoder block and demultiplexes it into many channels (including Control information)– some may be scrambled & the other may be free to-air programmes.

Question :- As per the DAS, there should not be any free-to-airprogram.

19) Page-24, Section-5.4 #b, II,

Message displayed by STB on TV contains SMS format to be sent to the operator along with the operator's number.

Question :- There are many MSOs (few thousands) and around 6/7 DTH operators in the country. So, it is not possible to store the message specific to each operator as there will be limitation in terms of Memory.

Suggestion :-There should be nodal agency and one toll free number who manages the activation process. However, the cost for such service should be free, else it will increase the overall costs.

20) Page -27, Section 5.4 #b, XVI,

The periodic key (PK) is only valid for "M" number of days (typically 15-30 days) as decided by operator or as conveyed through trigger message. User has to complete registration process after every M days.

Question :- This is very cumbersome process for the User and due to this user may avoid to take these STBs.

Question :- Can "M" number of days higher than 30 days? Can this value different as per the operator or it should be universal?

21) Page -25, Section 5.4 #b, XVII,

Operator also keeps track of validity of registration process for each user. Operator will send message to user to complete renewal process through SMS to registered mobile number as well as to the STB/smart card over the air.

Question :- This will increase the SMS load for sending the messages on mobile as well as on the STB. For messages on STB the EMM load will also increase.

Suggestion :- There should be automatic process for displaying the renewal message by STB based on the elapsed time after the successful registration process based on the "M" number of days decided.

22) What will be workflow in case user wants to switch from the DTH operator to the Cable operator?

23) How interoperability will be achieved in case of only one cable operator signal available in that region? The end-user would have ended up purchasing the STB but that investment would go waste if only one cable operator signal is available in that region.

24) Page-33, Section 5.5
cut-off date for removing the non-interoperable network elements.

Suggestion :- We suggest to keep using the existing implementation for the PSI/SI as it will be impossible to update all the STBs deployed in the field due to various reasons such as memory constraints, support from the manufacturers etc.
The new interoperable STBs should work as specified in the section 6.c.

25) Page-33, Section 5.5 - Standalone Games

Question :-. With this proposed framework, operators needs to carousel a second instance of the same Games and application to cater to the new framework while keeping the existing deployment untouched. This will result in additional Bandwidth.

26) Page-36, section 5.6 :- Secure Boot and OTA

Question :-It is not clear from the framework as to the number of STB manufacturers to be supported by the operator. This is required because the operator will need to carousel the STB software image continuously in the headend. Hence, if there are hundreds of STB model types than the operator will have to provision sufficient bandwidth to cater to hundreds of software images on air.

27) Page-44, Section 6.cTable 1 Point #3 - Service list and description

Question :- if the service_list_descriptor is not available in NIT, then STB SW has to tune to each TS and then build the service list. This will increase the Installation time.

28) Page-45, Section 6.c Table 1 Point #4 - Service categorization

Question :- The Content_descriptor is mainly used for the categorization of the EPG data (Events). It will be difficult to categorize the services based on this descriptor.

- It will increase the EPG data and due to this BW will also increase
- For some of the channels the events are very dynamic and due to this service should move from Movies to sports or to Entertainment.
- This will increase the STB SW complexity as service categorization needs to update in real time based on the events.