Sky UK response to TRAI consultation paper on “Interoperability of Set Top Box”

Foreword

Sky UK thanks the Telecommunications Regulatory Authority of India for the opportunity to respond to this consultation. Sky has no direct interest in the pay TV market in India hence we hope that this response will be considered to be from a commercially neutral position.

Sky UK is part of Sky Group, a company which has in excess of 23 million customers across European territories. The foundation for Sky Group from the early 1990s was Pay TV and the product and service portfolio now includes fixed and mobile telecommunications services including broadband. The motivation for Sky UK to respond is that interoperability, particularly in security systems, is an area of industrial technology that Sky UK has closely followed since the early 1990s. ECI has been one of the topics included in the scope of our activities, we have reviewed numerous documents and conducted our own analysis. We believe it is in the best interests of the Indian authorities and fellow pay TV stakeholders that we share some aspects of our analysis, hence this response.

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

A1. While the goal of full interoperability of STBs seems attractive to some stakeholders and regulators in enabling switching between service providers, in practice it means that interoperable devices have to include support for all the networks that they will be used on. This consultation focuses on interoperable security but several other technical aspects need to be considered to ensure interoperability – these will be mentioned later in this response. For this answer, we simply conclude that providing for interoperability will add cost to STBs. Retailed devices will become more expensive for all consumers which could have the effect of holding back innovation if the increased investment discourages consumers from upgrading to receive new services – operators may struggle to find a business case that supports new products. Operators that supply their own devices may lose the option of providing cost reduced STBs to suit specific business plans. The transitions from analogue to digital, from Standard Definition to High Definition, and so on, could all have been held back by regulations raising the cost of STBs.

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.

A2. The question only considers RF reception as an interoperability factor whereas there are other aspects involved in achieving interoperability such as interactive functionality, return path, security, networking to other devices etc. Including all this functionality for all platforms in a single STB would add a significant amount of cost which all consumers would have to pay but many would not want or need to. An alternative arrangement to a regulated environment which imposes costs on all consumers is a market led approach whereby fully interoperable products will be marketed if there is demand from consumers for them.

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

A3. It is unlikely that interoperable STBs would be voluntarily made available through any means other than an open or retail market. The incentive for platforms and service providers to provide such STBs seems hard to envisage as it would add significant cost for little or no commercial benefit.

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?

A4. The EC has considered this question carefully in recent years and has developed an Eco Design framework which focuses on ensuring that the scarcest resources in a product are re-used and that manufacturers take responsibility for the overall re-cycling of the products they produce. Power consumption is another area of focus for this framework. The EC has not regulated on interoperability of reception devices since the MAC Directive, which was subsequently rescinded because regulators had misjudged the market requirements. Another aspect that should be considered is the life-cycle of STBs. Interoperable STBs are typically retailed and retail devices are usually maintained (in terms of patches for security defects, vulnerabilities etc.) only for a year or two at most. If the security of a device which is no longer maintained is compromised, the device may be disabled through revocation and the consumer forced to purchase a new device, perhaps when it is only just over two years old. By contrast, operators are incentivised to maintain the STBs they supply for a much longer period, typically around ten years, which contains the environmental impact of replacement.
Our conclusion is that when considering how best to reduce environmental impact of a particular class of products, regulators should investigate alternative regulatory interventions through full commercial, life-cycle / re-cycling and general Eco analysis and justifications. Considering life-cycles and re-cycling may be more environmentally sound and more efficient for consumers, operators, competition and innovation than regulating on specific interoperability technology.

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

A5. The channels for distribution of content are diversifying rapidly beyond pure broadcasting. Forcing cable and DTH platforms to use the same STB platform will add cost and commercial uncertainty to the broadcasting of content and will damage its competitiveness and scope for innovation versus on-line content distribution (OTT) and cloud services such as storage and catch-up.

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.

A6. Please see the answer to Q8.

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

A7. This response does not recommend an interoperable solution for STBs. However, in the event that regulatory intervention is undertaken, any attempt to introduce an interoperable solution should be very carefully prepared and based on tried and trusted technology. Such technology should be created in open standards body groups in order to ensure wide industry acceptance and adoption. A compliance and robustness regime should have been created. In addition, if the technology has not already been adopted in the market, review of the technology coupled with the compliance and robustness regime by a competent professional body should be a condition for consideration. Work on a deployment plan should not begin until a specification has reached this more assured and tested status.

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.

A8

Commentary on software vs hardware solutions for security

Given that the focus of this question appears to be on security, this answer will focus on that single aspect of interoperability (although as already mentioned, there are many others). Effective security for pay TV content always requires some balance of hardware and software elements. A paramount consideration for security systems is that it must be possible to maintain, update and renew some of the elements in order to address the threat of hacking and piracy. Where a return path cannot be guaranteed, the device is required to bear the full responsibility for securing content. Hardware technologies must be utilised for CAS processing, key ladder processing and content decryption. Software solutions are not suitable for one-way systems. For systems which have a return path, a predominantly software solution can be safely utilised. In situations where a return path cannot be guaranteed, the device is required to bear the full responsibility for securing content. Hardware technologies must be utilised for CAS processing, key ladder processing and content decryption. Software solutions are not suitable for one-way systems. There are other considerations of course but the existence of a return path is a determinant for whether a predominantly software solution can be secure enough.
MovieLabs, an organisation supported by the major Hollywood studios, has produced a specification for Enhanced Content Protection now at version 1.2 (available from https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf) which demonstrates how the premium content providers are moving increasingly towards secure hardware elements in the fight against piracy.
Predominantly software solutions can be efficient if they provide effective security, but the cost of piracy cannot be over-estimated – it has caused numerous business failures; any weakness in a security system, particularly one with a large user base, will be ruthlessly exploited.
N.b. A key use case claimed for ECI is one-way systems with no return path.

ECI was conceived and specified from a very limited perspective

The concept for the ETSI GS ECI suite of specifications was crystallised more than a decade ago by a small group of individuals with a specific interest in the most extreme CA/DRM interoperability. A report was produced in 2010 which details the position of the contributors. However these individuals were not able to generate sufficient interest and support in creating a specification in one of the mainstream standards organisations that work in this area (e.g. ETSI, DVB), so the supporters of the ECI concept decided to form an ETSI GS group. ETSI's GS process is designed to enable small interest groups to create specifications for niche applications and markets.
The specification itself was completed over three years ago (2016). The working group that produced the specification was composed of a very small number of participants (fewer than 10) under terms and conditions of participation that were very restrictive.

There are some key concerns about lack of cross-industry involvement in the ECI specification creation process

There was only ever one security vendor involved in creating the specification. That security vendor declined to sign over its IPR to the ITU and has not supported the process of taking the ECI through ITU; it would appear that the security vendor involved has effectively walked away from the ECI suite. None of the other major security vendors that we have been in contact with believes ECI will provide a solution that is suitable for today's pay TV content protection needs.
There was only ever one manufacturer involved in creating the specification. If it made any contributions none of them resulted in any IPR being generated. The manufacturer was on the fringes of the CE market and now appears to have exited that market altogether. Mainstream mass market CE manufacturers that we have been in contact with do not regard ECI will provide a solution that is suitable for today's pay TV content protection needs.
There were never any silicon vendors involved in creating the specification. The scale of silicon requirements and the implications for existing SoC solutions have never been considered. These aspects have serious cost consequences.
Specifications intended for wide application are generally created in large, open groups because this brings more knowledge and expertise into play by securing representation across a wide cross-section of industry.

Broad agreement by a wide group of expert stakeholders is a required step towards mass market suitability and acceptance.

There are some key concerns about the unproven quality of the ECI suite of specifications

- *No test implementations for ECI have been produced, it is entirely unproven in practice.*
- *No review by a professional expert body (for example IET, IEEE etc.), has taken place. The limited review taking place in the ITU process is no substitute for a thorough, independent activity. If the full suite of ECI specifications is ever approved by the ITU, this will not provide any assurance of ECI's integrity and suitability for the pay TV market today.*
- *In 2018, the ETSI cyber security group (TC Cyber) turned down the opportunity to take the ECI specification into a full ETSI group. It can be presumed that the members of the group decided the ECI concept and suite of specifications were still unsuitable for a mainstream standards organisation.*
- *A review of ECI commissioned by Sky UK from an experienced security expert consultancy highlighted a large number of serious issues with ECI. This is available to anyone with access to the ITU TIES system at https://www.itu.int/md/T17-SG09-C-0106/en. A copy can be requested from martyn.lee@sky.uk.*
- *Within the ITU process, some improvements are being proposed for ECI, however without more scrutiny and input from security vendors, mass market manufacturers, silicon vendors and professional bodies, ECI cannot be considered to be a solution which can achieve a sufficient level of industry acceptance.*
- *Fundamentally, ECI is a dated realisation of an old concept which has a flawed architecture and does not take account of the counter-measures needed against today's and tomorrow's threats of hacking and piracy.*
- *Three examples (of many) of ECI's shortcomings are that a) it lacks the capability to introduce secure forensic watermarking and b) it has a fully standardised download system (DVB's security experts group specifically warns against this kind of architecture), c) it introduces common security components into all devices which reduces diversity and increases the risk and impact of an attack on the system.*

To regulate in favour of ECI adoption, whether for one sector of the broadcast market or all, without the following having been done in advance:-

- *development of compliance and robustness (C&R) rules applicable to the Indian environment,*
- *establishment of strict warranties and liabilities for security breaches,*
- *proper expert professional review, including the C&R,*
- *proof of concept testing involving at least two security vendors,*
- *full cross-industry scrutiny and acceptance,*

would carry extreme risk for all stakeholders involved.

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?

A9. Setting up a Trust Authority is a costly and complex process, not necessarily economically viable in its own right, and beyond the scope of a consultation response to describe in any detail. A few brief comments follow:-
The preparation of compliance and robustness rules is a highly specialist pre-requirement for the Trust Authority to work effectively. The Trust Authority has to be able to ensure that all devices meet and are tested to the standard required, to ensure that the Trust Authority only certifies compliant devices and weak implementations do not reach the market. All parties involved need to agree to the policies and processes of the Trust Authority. As the only body with a relationship with all stakeholders, a Trust Authority would need operational capability and may need to have an operations centre to deal with incidents.
A limited number of industrial organisations and bodies have shown themselves to be capable of implementing this kind of operation.

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.

A10. Please refer to the responses to Q7 and Q8 and see the summary below.

- *development and selection of security technology developed and approved / determined in a truly open standards environment,*
- *development of any ancillary specifications that the required level of interoperability depends on,*
- *development of compliance and robustness (C&R) rules applicable to the Indian environment,*
- *establishment of strict warranties and liabilities for security breaches,*
- *proper expert professional review, including the C&R,*
- *proof of concept testing involving at least two security vendors,*
- *full cross-industry scrutiny and acceptance,*

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?

A11. If interoperable solutions can be introduced, and this is highly questionable, it will only assist competition in the retail market for STBs. It is likely to damage competition between platforms and hamper innovation. In the event of a wholly retail market for STBs, the launch of new products and services to consumers is likely be more difficult to achieve and more protracted. Competing with the more agile on-line content distribution companies will be more difficult.
There is a litany of failed attempts to establish devices with interoperable security into the retail market. The US CableCard is perhaps the most prominent example, see for example https://en.wikipedia.org/wiki/CableCARD. As a recent example, YouView devices in the UK have also failed to become established as a retail market proposition although YouView STBs are available from platform operators.
As previously mentioned, establishing a suitable period of maintenance, at least on security aspects, for devices distributed via the retail market, c10 years, rather than the usual 1 to 2 years, is a major challenge.

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?

A12. Interoperability between platforms and service providers can already be achieved through various means. For example, DVB Simulcrypt allows the services of one platform to be received and decoded on the STBs of another platform. The MPEG Common Encryption solution (MPEG-CENC) provides for one piece of content to be received and decoded on a variety of multimedia players. DVB CI-Plus has now been enhanced to version 2 which allows the cheaper USB interface to be used. These are all tried and trusted solutions for interoperability of security. None of these solutions, could be applied to legacy devices without the specific hardware components required to deploy them. Nor could ECI.

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

A13. None.

Submitted by Martyn Lee Sky UK 9th December 2019