Telecom Regulatory Authority of India

सत्यमेव जयते

Pre-Consultation Paper

On Set Top Box Interoperability

4th April, 2016

Mahanagar Doorsanchar Bhawan

Jawahar Lal Nehru Marg

New Delhi- 110 002

Website: www.trai.gov.in

CONTENTS

Written comments on the Pre-Consultation Paper on Set Top Box interoperability are invited from various organizations, industry bodies, standardization bodies, STB manufacturers, chip vendors, Conditional Access System providers, software providers, stakeholders, experts, individuals etc. by 29th April, 2016. The comments may be sent, preferably in electronic form to Mr. Sunil Kumar Singhal, Advisor (B&CS), Telecom Regulatory Authority of India, on the e-mail:- sksinghal@trai.gov.in or gs.kesarwani@trai.gov.in . For any clarification/ information, Mr. Sunil Kumar Singhal, Advisor (B&CS) may be contacted at Tel. No.: +91-11-23221509, Fax: +91-11-23220442. Comments will be posted on TRAI's website www.trai.gov.in.

Chapter-1

Introduction

1.1 India has a large base of pay TV subscribers. Predominantly, the pay TV services are being delivered through Cable TV and Direct to Home (DTH) systems. Other modes of TV broadcasting such as Internet Protocol TV (IPTV), Head-end In the Sky (HITS) have miniscule subscriber base as compared to the Cable TV and the DTH systems. There are 6 pay DTH operators, 2 IPTV operators, 2 HITS operator and large number of Multi System Operators (MSOs) providing TV services through Addressable Systems in the country.

1.2 The reception of the Cable TV services (provided through Digital Addressable Systems) and DTH services requires a Customer Premises Equipment (CPE) which is connected with the TV set. In DTH the CPE comprises of a Set Top Box (STB), a small Dish antenna along with LNBC and RF cable; where as in Digital Cable TV services, the CPE comprises of STB only. Presently the CPE (mainly the STB) of a particular operator installed at the premises of a subscriber cannot be used by the subscriber for reception of signals of the other operators. In such a scenario, every time when a subscriber wants to avail the services of the new operator he buys again a new STB. This phenomenon is referred to as non-interoperability of STB. STB is non-interoperable and is tied to specific operator due to various technical, commercial and market driven reasons. The commercial implications of non-interoperability of STBs are huge. As per the report submitted by DTH Operators to TRAI, as on December 2015, around 85 million of STBs have been either sold or provided to the subscriber in the market, out which only around 55 million are in active mode. This indicates that around 30 million STBs are lying idle or unused, mainly because of non-interoperability of STBs.

Since the inactive STBs cannot be used for reception of services of the other operator, the money invested into the STB go waste and it also results in e-waste. Considering an initial capital expenditure around $ 25 per STB, a total of $ 750 million capital is lying unused. The exact data in respect of Cable TV services is not available but it is anticipated that the numbers of inactive STBs are very large.

1.3 Interoperability of CPEs plays an important role for the growth of any sector. Consumers have today tasted the freedom due to interoperable mobiles and Personal Computers. It is difficult now to visualize a locked world in broadband and mobile services. But, the same is not the case with STBs. The same STB cannot be used interchangeably across the different service providers. Although all STBs used for pay-TV services perform essentially the same functions – they remain distinct from each other, as if they were different equipment. The non- interoperability of STBs between different service providers has not only compromised the competition in the Pay-TV market but also a major hindrance to technological innovation, improvement in service quality and sector growth. Besides this, the Operators have been claiming that they are giving huge subsidy to the consumers for providing STBs; the interoperability of STBs will also reduce the burden of subsidy to great extent.

1.4 TRAI has taken up the issue relating to development of interoperable STBs in Digital Television Broadcasting sector that should be compatible across various platforms. STB interoperability would empower the consumers to change their cable TV (or DTH) service providers whenever required, without changing their STBs and without any major cost implications. This would shift the focus of the sector towards providing better quality of services to the consumers at competitive prices.

Implementation of STB inter-operability, will also make them available in the open market, will drastically reduce cost, and address the challenge of e-waste resulting due to discarded set-top-boxes. Availability of set-top-box in open market will reduce capital requirement of service providers and improve the cash flow position of the industry.

1.5 The Authority has decided to issue pre-consultation paper to identify various issues related to interoperability of STBs, challenges and concerns of the industry. Chapter 2 of this paper provides details of TV signal transmission and reception in Digital TV as per Digital Video Broadcasting (DVB) standards. Chapter 3 gives a snapshot of International Scenario on technical interoperability and chapter 4 discusses the issues relating to STB interoperability.

1.6 Comments of various organizations, industry bodies, standardization bodies, STB manufacturers, Chip venders, Conditional Access System (CAS) providers, software providers, stakeholders, experts, individuals etc are solicited so that various issues can be identified and suitable solutions to implement STB interoperability can be worked out.

Chapter-2

Signal Transmission and Reception in Digital TV

(As per DVB Standards)

2.1 In Digital TV the signal transmission from the MSO/DTH head-end to the subscriber STB involves a number of processes which ensures error free and secures transmission. At the transmitter end, the base band audio-visual signal is compressed using MPEG standards. The compressed signal is then scrambled to ensure that only the intended users are able to view the signal after descrambling. The multiple programs are multiplexed using a multiplexer to form a transport stream (TS).The control word (CW) used for scrambling purpose is also transmitted in encrypted mode along with the TS. The TS is modulated for transmission purpose using the DVB standards. The signal is then uplinked to KU band Satellite for DTH for direct reception by the subscribers. In Cable service the signals is converted into optical mode and transmitted thorough optical fibers and Coaxial RF cable as last mile connectivity to the subscribers.

The diagram shown below (Fig. 1) provides an overview of the transmission system.

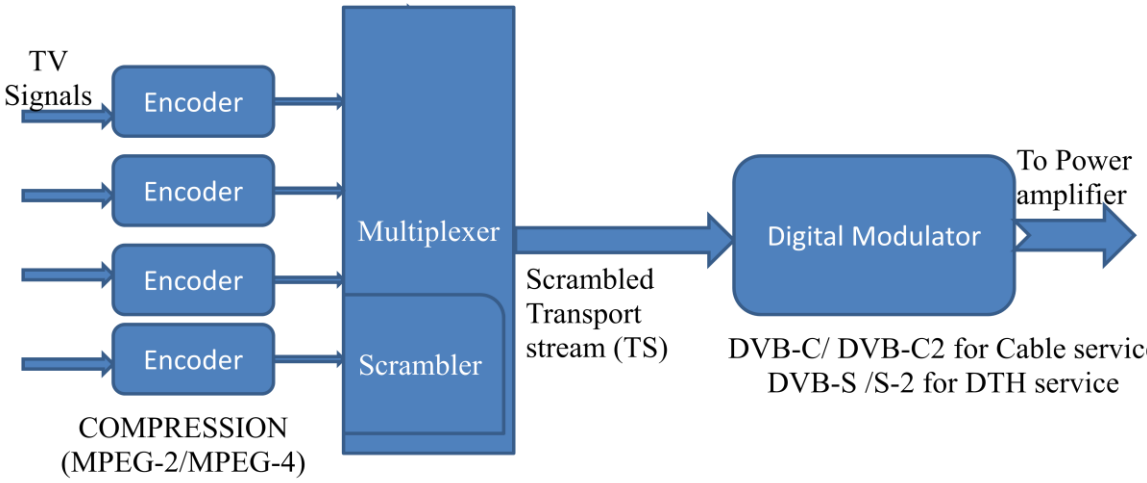

Figure 1: Signal Processing at Transmitter end

2.2 At the receiver end the signal is captured using dish antenna in case of DTH services and through Co-axial cable in cable networks. Front end in STB consists of tuner and demodulator. The tuner tunes the signal and passes the required band of signal to the succeeding modules of the STB. The hardware configuration of all STB is generally same up to demodulator, which is different for different DVB receivers as their transmission schemes are different. The demodulator demodulates the signals. The demodulated signal is then descrambled using the same CW which was used for scrambling the content. The descrambled signal is then decompressed using MPEG decoders which may again be different depending on the coding scheme used.

2.3 Scrambling of the compressed data is done according to a standard as specified by DVB, known as Common Scrambling Algorithm (DVB-CSA). During Scrambling, 2 messages are added to the TS namely, Entitlement Control Message (ECM) & Entitlement Management Message (EMM). ECMs are added to TS on per channel basis. It contains the CW which is used to scramble a program. ECM also includes the channel ID and the time and date information which allows the STB to know what the current time is and to make a decision if the user is allowed to watch the channel or not. ECM is encrypted in a proprietary way by Service Key (SK).

2.4 EMM is unique for each subscriber. It carries a list of channels which the owner of that STB is entitled to view and also the date up to which he is entitled to receive them. The EMM also carries the SK of ECM. EMM is also encrypted in a proprietary way by Public distribution Key (PDK). PDK is unique for each customer. The smart card of STB contains this PDK. In card-less STBs, the PDK is configured in the STB itself.

2.5 The encryption of EMM and ECM are done in a proprietary basis. This is the root cause of non-interoperability.

2.6 For descrambling the channels, EMM and ECM are extracted separately From the TS. When an EMM is received, it is decrypted by PDK available on the smart card or on STB. The list of entitled channels to the consumer is then gets stored in the internal database of the STB. Along with EMM, SK also becomes available. ECMs are decrypted by SK. The information provided by ECM viz time and date information, channel ID with the help of internal data base are used to decide if the user has access to the channel or not. If the user has access to the channel then the CW is sent to the descrambler of STB which can then descramble the channel. Figure 2 shows the complete signal transmission and reception functional blocks.

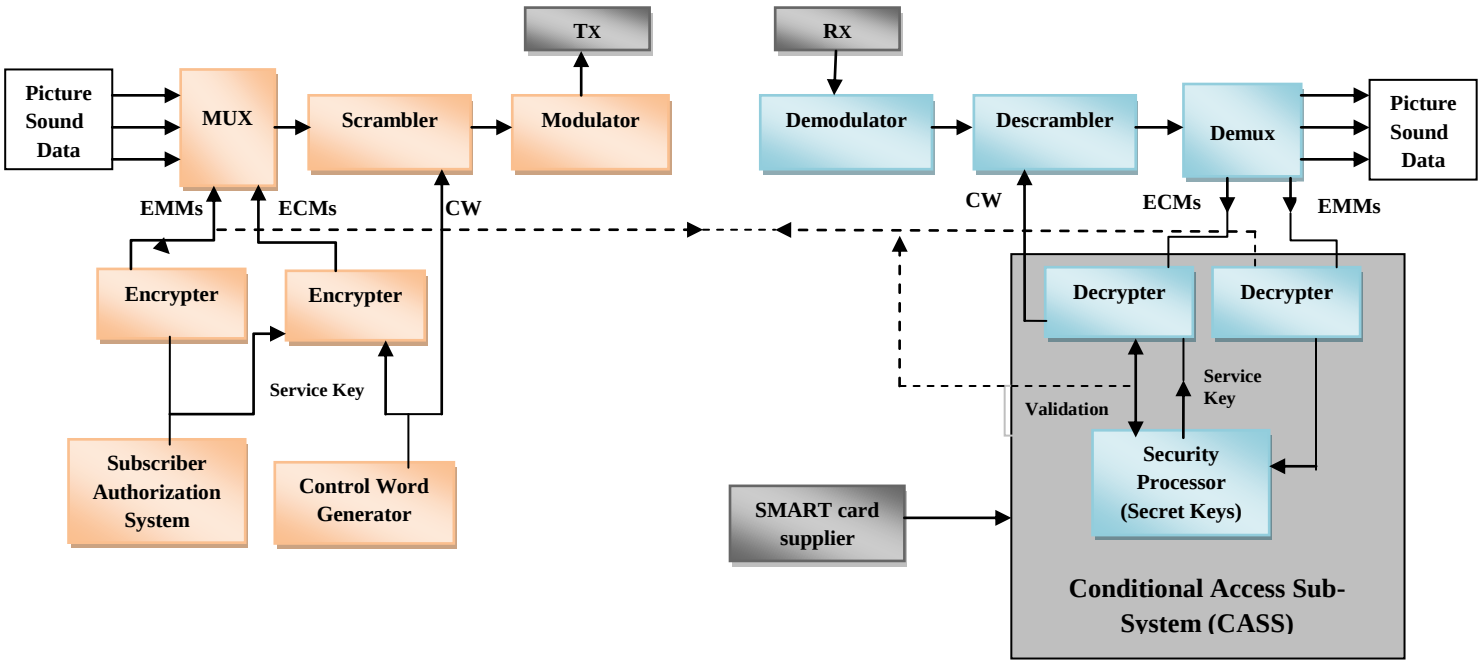

Figure 2: A snapshot of complete Signal Transmission & Reception

2.7 The current business model used in Pay- TV systems follows a circle of dependency, wherein DTH operator/ MSO, CAS vendor and STB manufacturer have to work in a restricted vertical market. In this model, a STB manufacturer needs to pay licence fee to CAS vendor, in order to use CAS in his STB and sign a non-disclosure agreement with the CAS vendor in order to enable his STB to work under security considerations adopted by this CAS. The subscriber is compelled to use the specific STB pre-determined by the operator; as such he cannot access his entitlements via any other STB or receive contents from any other operator.

Chapter 3

International Scenario

US approach:

3.1 *Cable Card:* In the year 1998, the Federal Communications Commission (FCC) issued an order which mandated a conditional access element separate from STB, in order to permit unaffiliated manufacturers and retailers to manufacture and market STBs while allowing digital addressable platform operators to retain control over their system security. It led to development of The Cable Card in the year 2003.

3.2 The Cable Card, is a security device (similar to a credit card) provided by an operator, and it can be inserted into a STB or TV set by a consumer enabling the consumer's TV to display operator encrypted video programming. In 2005, the FCC prohibited operators from integrating security functions into STBs which was later extended to 1st July 2007. However, attempts by the FCC for ensuring commercial availability of third party STBs could not make much material impact, as from 1st July 2007 till April 2010 only 0.45 million Cable Cards were sold whereas leased STBs (having inbuilt Cable Card) during this period were 17.7 million. FCC has recognized that in effect the Cable Card approach (i.e. having STB and Cable Card from independent sources) has not been able to achieve its objective. FCC identified two fundamental defects in this regime - with few exceptions, retail STBs were unable to provide functionality in comparison to the STB leased by the Operators. The subscribers were often unable to access many of the operator's services that leased STBs used to provide. The commercial success of the Cable Card is very limited.

3.3 *Downloadable Conditional Access System (DCAS):* In reaction to the Cable Card failure, the US cable industry had established a project for development of a DCAS, which would overcome the need for the Cable Card and would allow the cable operators to swap more easily their CA-system in case of security problems or in case they want to change to a different CAS vendor.

3.4 DCAS, as envisioned, removed the need for physical set-top boxes or Cable Cards to protect encrypted digital content. It was proposed that instead of a card with removable circuitry, a custom ASIC chip could be soldered onto the circuit board of any digital cable-ready device. DCAS software would then run on this custom chip. Additional circuitry needed to run the OCAP (Open Cable Application Platform) operating system would be required. OCAP programs then would be used as the sole method of interacting with DCAS since it will enable cable companies to force the download of new security software. As set-top box ASICs have now advanced to SoC implementations, the minimum hardware circuitry to store key ladders (K-LAD) is embedded in the silicon, enabling much of the security functions to be implemented in software. Further, just as traditional set-top box functionality such as user-interface and middleware are moving to the cloud, DCAS enables much of the security functions also to move to the server side or the cloud. This allows thin client set-top boxes to be deployed that can be remotely managed, in lieu of the more expensive Cable Card based systems. An allegedly working DCAS prototype was created by Samsung and NDS for the cable industry and was demonstrated to the FCC in November 2005.

3.5 The DCAS-project was terminated in 2009 for various reasons (it may not have satisfied FCC requirements that security modules be separable, and required an operating system (OCAP) that a majority of consumer

electronics (CE) manufacturers did not wish to implement) before the development work had been finalized.

3.6 *Downloadable Security:* Recently the FCC has focused on downloaded security that would enable any set-top device to connect with and navigate any pay-TV service, regardless of type, by downloading the appropriate conditional access and content security software. For this purpose, the Downloadable Security Technology Advisory Committee (DSTAC) was created as a result of the Satellite Television Extension and Localism Act Reauthorization (STELAR) bill that was passed in December 2014. The committee has proposed an apps-based approach where Pay-TV operators and online video distributors would create both platform-specific apps (Android, iOS, Xbox, PlayStation, Roku, etc.) as well as HTML5 web apps that could be downloaded and run on virtually any connected device, including smart TVs. These recommendations of the committee have been submitted to the FCC recently and FCC has initiated consultation with stakeholders.

European approach:

3.7 *Digital Video Broadcast (DVB) Common Interface (CI):* One of the first exchangeable Conditional Access/ Digital Rights Management (CA/DRM) solutions introduced by DVB (Digital Video Broadcast) group to the European broadcast area was Common Interface (CI), making it possible to change a CA/DRM system by change of a Conditional Access Module (CAM) together with a smart card, issued by a specific service provider. With some further improvements, covering e.g. the encryption between module and host, the next generation of common interface, known as CI+, was specified and developed. This industry specification, including a trusted environment, soon was accepted by the market participants, although not been developed by DVB as an ETSI (European

Telecommunications Standards Institute) standard but instead as an industry specification by the CI plus consortium. The overview of these developments is provided below:

i. In 1997, The DVB CI Standard was created to specify a TV PCMCIA module as a plug in equipment for TV receivers to descramble the encrypted TV channels. Once descrambled, the module is sending back the program to the TV. The interface between TV and module is named the Common Interface.

ii. In 2002, European Union mandated all Digital TV sets with screen larger to 30 cm to be fitted with Common Interface. Europe was at that time preparing the Terrestrial Analog Switch Off that triggered TV replacement for users in most countries. It allowed population to keep the freedom to switch between operators and services without having to replace their equipments.

iii. In 2007, CI Plus (CI+) forum was created by 4 TV manufacturers (Samsung, Panasonic, Sony and Philips) and 2 modules manufacturers (Neotion, SmarDTV) with the objective to evolve the DVB CI standard to enhance copy protection on the common interface.

iv. In 2009, the CI Plus Specification V1.2 was released, as an open standard by CI+ LLP (Limited Liability Partnership group with members Sony, SmarDTV, Samsung, TPVision, Panasonic, Neotion and SMiT). In 2011, the CI Plus Specification V1.3 was released and transferred the responsibility of standard evolution from LLP to DVB. The diagram in fig – 3 shows the concept.

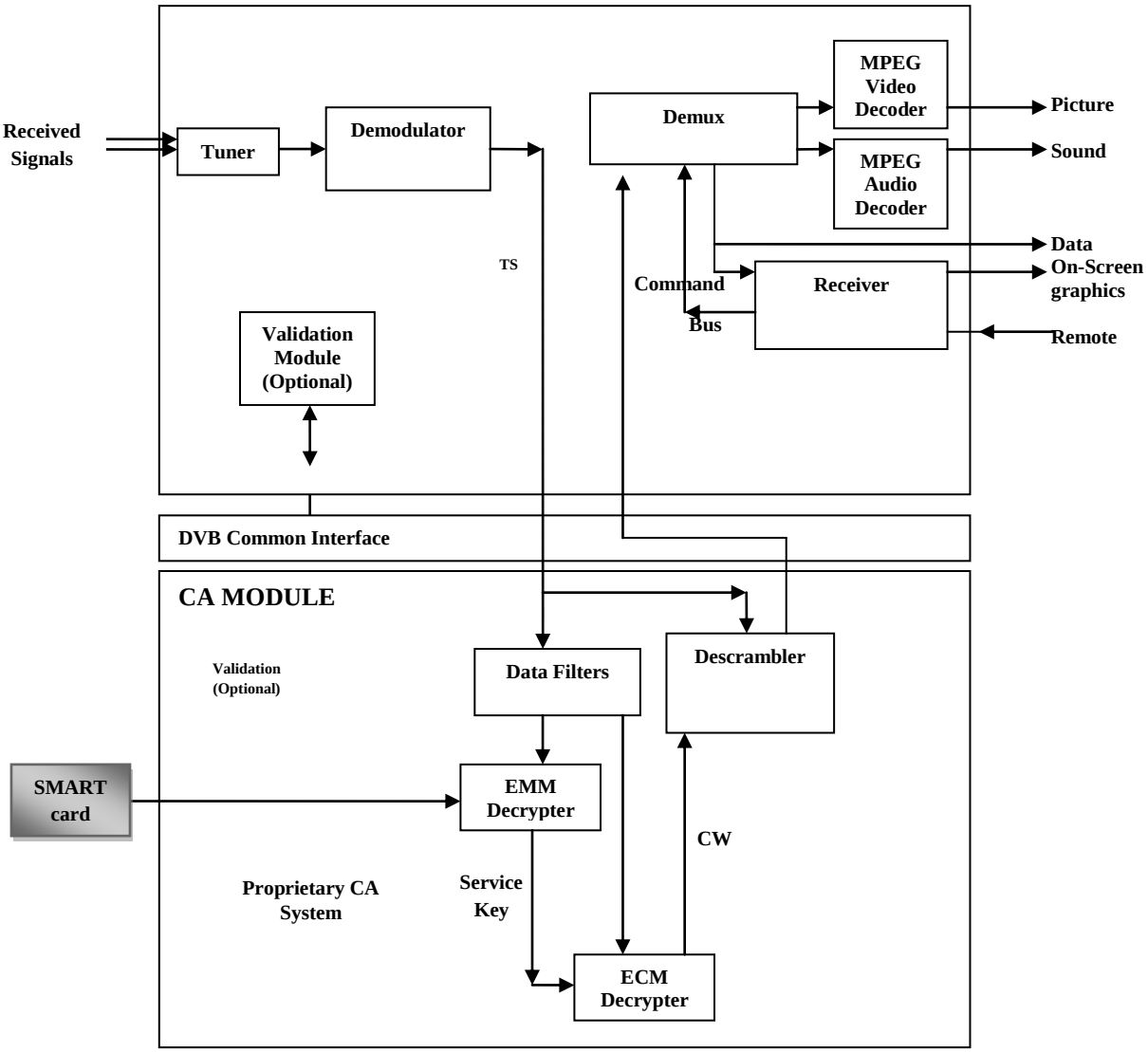

Figure 3: STB with DVB-CI Interface

3.8 Despite the fact, that CI+ might be regarded as an evolutionary step, shortcomings still remain, as this technology keeps relying on hardware modules with a list of disadvantages as e.g. rather high production cost, currently only one active CA/DRM system at a time, solution only for broadcast content, necessary hardware change in case of update by service provider and not addressing mobile and smart devices in multi screen scenarios.

3.9 DVB will be coming out with a new versions of the CI Plus specification that is, DVB CI+ 2.0. In addition to new features and functionality, the current PCMCIA base physical form factor will be replaced by a more compact interface solution (CI Plus 2.0).

3.10 *Embedded Common Interface (ECI):* ETSI has launched a new Industry Specification Group (ISG) on Embedded Common Interface (ECI) for exchangeable CA and DRM solutions in 2014. The work of this ISG is to consider a standardized environment for a general purpose, software based, embedded, exchangeable CA/DRM system. These standards should allow consumers to be able to continue using equipment and content they have previously paid for, after a move or a change of network provider, or access content from multiple service providers using the same device.

3.11 This group has proposed software based embedded, exchangeable CA/DRM system. Key benefits of the envisaged approach for content security are:

- Flexibility and scalability due to SW based implementation,
- Applicability to content distributed via broadcast and broadband, including OTT,
- Support of multi-screen environment,
- Opening of the market by avoiding "Lock-in" for platform operators, network/service providers, and consumers,
- Open entire eco-system fostering market development.

3.12 The core element of ECI is to specify the interface between the software-based CA/DRM –client and the host system. Therefore, amongst others, the ECI has the following functionalities:

- A software container for the CA respectively the DRM kernel – hereafter called ECI Client with:
  - Standardized interfaces to all relevant functionalities of the CPE

- A standardized Virtual Machine (VM) to run upon

- Support of smartcard-less systems as well as use in smartcard-based systems
- Inclusion of a multitude of such software containers in a CPE, each container running on its own instance of the VM
- Installation of the ECI Client independently from other CPE software by a secure and standardized loader concept
- Advanced Security, also known as Chip Set Security, to support state-of-the-art content protection
- Provisions to leverage hardware-assisted security functionalities
- Methods for the user to discover the right ECI Client to download
- Methods for revocation of (parts of) the ECI Client's functionality and CPE's functionality
- Suited for classical digital broadcasting, IPTV or modern OTT-based systems.

3.13 The complete specifications of ECI are not released yet, the standardization activities in ISG ECI will focus on a future-proof, advanced embedded solution, making hardware-based CAMs obsolete, and being fully specified as a SW solution.

3.14 Also, in Europe, for giving interoperability to the DTH boxes, the DVB simulcrypt standards are followed for interoperability requirements for the Digital Head-ends.

Asian Approach:

3.15 Singapore (Infocomm Development Authority, IDA) and Media Development Authority (MDA)) has initiated an Industry dialogue under the term "Next Generation Interactive Multimedia, Applications and Services – Project NIMS" in 2009, addressing, beside other aspects, the needs to identify common interfaces for the functionality of advanced STBs. The idea behind the so-called "Common featured Set-Top-Box" is a concept based on common features with standards-based technical specifications and open interfaces for all involved STB devices. This concept also allows optional features for differentiation from service provider´s view as well as end-user´s access to various network and service providers and their content, based on a flexible advanced Retail STB.

3.16 Singapore's telecom and multimedia regulators decided to drop this search for a standardized pay-TV set-top box, due to technical and business constraints which prevented some of the proposals from gaining traction.

3.17 Several further activities from Asian countries have led to several new work items in the area of CA/DRM systems; currently e.g. ITU-T is working on Draft Recommendations on renewable conditional access client software (initiated by ETRI, Korea) as well as on DRM standardization, concerning hybrid scenarios (initiated by Japan CableLabs).

Chapter 4

Issues relating to STB interoperability

Issues

4.1 Broadcasting of TV signals over distribution networks involves various steps like compression, encryption, transmission etc. For each purpose, different-different technologies and their versions have evolved over a period of time. The rules and regulations prescribed by the Government and the Regulator provide freedom of choosing technology to service providers. Accordingly, as per their business plan, individual service provider has chosen and implemented different technologies and their versions. The adoption of different-different versions of technical standards by service providers is one of the reasons for non –interoperability of STBs.

4.2 The issue relating to technical interoperability mainly hover around the question of interoperability of STBs, between two platforms viz DTH and Cable; and question of interoperability of STBs within the same platform i.e. with in Cable or DTH systems. Further, within a platform, there could be a question of interoperability of STBs across the different service providers using the same make of CAS. Presently, STB interoperability is not functional at any level.

4.3 Main technical reasons of STB Non-interoperability can be attributed to the following reasons:-

4.3.1 Different methods of EMM & ECM encryption: ECM and EMM messages are carried in an encrypted form. Whereas DVB has standardized the scrambling algorithm for scrambling of a channel (DVB-CSA), algorithms used for ECM/ EMM encryption are not standardized.

4.3.2 Different Modulation standards: The signals are modulated before transmission. In cable the signal is modulated using DVB-C standard whereas the signal is modulated using DVB-S standard in DTH. For a STB to be able to receive signal both from DTH and cable, there will be a requirement of switchable demodulator unit. Further, efficient versions namely DVB-C2 and DVB-S2 have been deployed by the operators. While the later versions are backward compatible, earlier versions are not forward compatible. Therefore, it restricts the STB interoperability across the platforms as well as within the same platform using different versions of standards.

4.3.3 Different compression standards: In digital TV transmission, compression plays a very important role. There are two prominent compression standards in use today. In India, most of the operators have used, either MPEG2 or MPEG4 standard for compression. In cable TV sector, due to cost advantage and availability of sufficient bandwidth in the network, most of the STBs deployed till now are of MPEG2 standard. While the MPEG4 standard is backward compatible, MPEG2 standard is not forward compatible. Therefore, MPEG2 compliant STBs cannot work in the MPEG4 networks.

4.3.4 Operating System/ Middleware and EPG (Electronic Program Guide) Boot loaders are specific to chip vendors and it allows the updating of STB software by specific operators after proper verification. There is no standard operating system for STBs. DVB has developed Multimedia Home Platform (MHP) as a standard for middleware. However the same is not popular. Proprietary middleware, with non-standard APIs, are in use. It ensures that, the application software can be updated by specific operators only. Special end user applications like EPG installed over middleware are also unique for each operator.

4.4 The pay TV service providers are concerned about the piracy of content. They have expressed their apprehension about fake STBs that may be used to capture information from a valid smart card and that information may be misused to produce fake/clone smart cards. Further, the stakeholders have raised their concern about the common scrambling algorithm (DVB-CSA) which is a 48 bit scrambling mechanism, and can be broken with the help of high capacity processors. Therefore, the service providers are reluctant to use DVB-CSA. Operators due to the concerns of piracy make the STB tightly coupled by integrating the Conditional Access Sub System into the chip.

4.5 All these becomes an impediment when a subscriber wishes to migrate to a different service provider while attempting to use the same STB, and leads to concerns relating to technical interoperability.

Steps Taken by TRAI for interoperability of STBs:

4.6 Interoperability of DTH STBs: Based on the recommendations of TRAI, for technical interoperability of STBs, the Government has mandated the provision of CI slot in the STBs deployed by DTH service providers. The CI slot exists in the already deployed DTH STBs. However this effort has not been fruitful in meeting the objective of interoperability in India due to various reasons, some of which are captured below :-

i. The availability of CI slot alone is not sufficient to achieve effective technical interoperability as other modules of STB like tuner, middleware, Operating System; EPG etc. also require updation on change of service provider.

ii. DTH operators are following different versions of standards for compression, and transmission.

iii. Most of the DTH operators have not offered to customers the option of CAM card in place of STB.

iv. The cost of CAM card is more or less equal to the new STB. It may be due to non-availability of economies of scale.

4.7 Commercial interoperability of STBs: TRAI has notified Tariff Order prescribing Standard Tariff Package for STBs, which provide an easy exit option to the consumers, who want to change their service providers due to one reason or the other. The Tariff order, applicable for DTH is sub-judice.

4.8 There can be various possible solutions. However, before starting any discussion on the possible solutions, it will be desirable to seek the comments of the stakeholders on various issue of the concern, likely methods to ensure set top box interoperability, common minimum agreement of adoption of any specific standards and the way forward. Some basic issues have been raised in this pre-consultation paper. However, stakeholders are free to give any relevant feedback for the development of technical interoperability both within specific segment (Cable TV and DTH) and across the segments (Among Cable TV and DTH operators).

4.9 A propos the above, the issue for consultation is:

i. In your opinion, what are the concerns that should be taken care of at the time of development of framework of interoperable of STBs?

ii. What are the techno-commercial reasons for non-interoperability of STBs other than those mentioned above? Please provide reasons with full details.

iii. What are the plausible solutions for technical interoperability of STBs and their impact on the sector growth?

iv. Any other issue which you feel will be relevant for development of technical interoperability of the set top boxes.

List of Acronyms

Abbreviations	Description
ASIC	Application-Specific Integrated Circuit
CAM	Conditional Access Module
CAS	Conditional Access System
CE	Consumer Electronics
CI	Common Interface
CPE	Customer Premises Equipment
CSA	Common Scrambling Algorithm
CW	Control Word
DCAS	Downloadable Conditional Access System
DRM	Digital Rights Management
DSTAC	Downloadable Security Technology Advisory Committee
DTH	Direct To Home Systems
DVB	Digital Video Broadcasting
ECI	Embedded Common Interface
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Program Guide
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
HITS	Head-End In The Sky
IDA	Infocomm Development Authority, Singapore
IPTV	Internet Protocol TV
ISG	Industry Specification Group
ITU	International Telecommunication Union
K-LAD	Key Ladders
LNBC	Low-Noise Block Down Converter
MHP	Multimedia Home Platform
MPEG	The Moving Picture Experts Group
MSO	Multi System Operator
NIMS	Next Generation Interactive Multimedia, Applications And Services
OCAP	Open Cable Application Platform
OTT	Over-The-Top
PCMCIA	Personal Computer Memory Card International Association
PDK	Public Distribution Key
RF	Radio Frequency

SK	Service Key
STB	Set Top Box
STELAR	The Satellite Television Extension And Localism Act Reauthorization
TRAI	Telecom Regulatory Authority Of India
TS	Transport Stream
VM	Virtual Machine

*****