Telecom Regulatory Authority of India

Consultation Note on Solution Architecture for Technical Interoperable Set Top Box

Dated the 11th August, 2017

The Telecom Regulatory Authority of India (TRAI)
Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg,
New Delhi – 110002.
website: www.trai.gov.in

1. The digital TV broadcasting services can be received by a subscriber using Set Top Box (STB) which is connected with the TV set (sometimes the STB is in-built in the TV set). The STB receives TV signals from distribution network and decodes them into viewable form on a TV set. STB enables the subscriber to view only those TV channels which he/she has subscribed.

2. Cable TV and Direct-to-Home (DTH) platforms are the major distribution platforms for delivery of TV broadcasting services in India. Whereas, the DTH services delivered in digital mode since beginning, the migration of cable TV services, from analogue to digital, has also been completed with implementation of Digital Addressable Cable TV systems (DAS) in the country.

3. Presently, Distribution Platform Operator (DPO) provides STB, which is compatible with his network to provide services to subscriber. Over a period of time, variety of technologies has been deployed by DPOs into the networks. It has led to a situation where STBs provided by one operator are not compatible with the system of the other operator. Some of the reasons for non-interoperability of STB are given in **Annexure-A**. This impedes portability of a subscriber from one operator to another in case he wishes to do so.

4. The lack of technical interoperability of STBs between different service providers has adverse effect on competition and service quality in the Pay-TV distribution market. Non availability of STB in an open market is also a major hindrance to technological innovations. Whenever, a consumer changes its service provider, the STB of existing service provider becomes useless as the same STB cannot be used; resulting into electronic waste (e-waste). The availability of practical solution which can provide technical interoperability of STB is always desirable.

5. The framework of interoperable STB should ensure the following:-

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

6. The Telecom Regulatory Authority of India (TRAI), *suo motu*, has taken up the issue of technical interoperability of STBs. In this regard, TRAI earlier issued a pre-consultation paper on 4th April 2016 to solicit the views of stakeholders to identify various issues relating to technical interoperability of STBs, challenges and concerns of the industry. The said paper was released with intent to drive the focus of the TV broadcasting industry towards the suitable solutions for technical interoperability of STBs, which can be worked out. In response to the pre-consultation paper, a total of 28 comments were received from stakeholders. These comments are available on TRAI's website www.trai.gov.in.

7. To address the concerns of the stakeholders in respect of interoperable STBs, as communicated in response to the pre-consultation paper mentioned above, TRAI collaborated with IIT-Bombay and Centre for Development of Telematics (C-DOT). The issues identified by stakeholders in response to the pre-consultation paper were communicated to C-DOT and IIT-Bombay. Now C-DOT, the telecom technology development centre of the Government of India, in close coordination with TRAI, has developed a solution for interoperable STBs. Describing the same, C-DOT has provided TRAI, a copy of the document titled "C-DOT framework and feature requirements for the ecosystem entities towards implementation of STB interoperability framework" which is attached with this document at **Annexure-B**.

8. Through this consultation note, TRAI presents the solution architecture for technically interoperable STB to all the concerned stakeholders to seek their comments on proposed solution.

9. In line with principles of transparency, this consultation note along with solution architecture document is being uploaded on TRAI's website www.trai.gov.in at URL http://www.trai.gov.in/release-publication/consultation. All stakeholders which include CAS providers, SoC vendors, middleware providers, EPG solution providers, STB manufacturers, Smart Card providers, and service providers like Broadcasters, Multi System Operators, and DTH Operators are requested to provide their written comments on the proposed solution architecture for technical interoperable STB by 25th August 2017. Comments will be posted on TRAI's website. The comments may be sent, preferably in electronic form to Shri Sunil Kumar Singhal, Advisor (B&CS) TRAI, on the e-mail:- sksinghal@trai.gov.in or gs.kesarwani@trai.gov.in .

10. Subsequently, TRAI is planning to organise a workshop on proposed solution architecture for technically interoperable STB during 1st fortnight of September 2017, to elaborate in detail on various technical aspects commented upon by the stakeholders in response to this consultation note. The date and venue of the workshop will be intimated later on. The stakeholders willing to participate in the workshop may register themselves on TRAI website. [The registration page can be reached by landing on Home Page ⇨ Workshop ⇨ Registration]. After incorporation

of comments received from the stakeholders and the said workshop, TRAI will be launching a pilot project on STB interoperability. Entities interested in pilot projects for deployment of Interoperable STBs can also send their details to TRAI.

11. For any clarification/ information, Shri Sunil Kumar Singhal, Advisor (B&CS) may be contacted at Tel. No.: +91-11-23221509, Fax: +91-11-23220442.

Annexure-A

Reasons of technical non-interoperability of STBs

1. The delivery of digital TV broadcasting services involves various steps like compression, encryption, modulation 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 of India and the Authority provide a flexibility of choosing technology by the 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.

2. Some of the reasons, of STB Non-interoperability, can be attributed to the following :-

a) **Different methods of encryption of EMM & ECM**: In DVB, CAS standards define a method by which a digital television stream can only be accessed by those entitled having valid decryption keys. This is realized by a combination of scrambling and encryption. Entitlement Management Message (EMM) containing list of pay TV services and duration and the Entitlement Control Message (ECM) carrying control word (CW) is transmitted along with the scrambled channels. ECM and EMM messages are carried in an encrypted form. Whereas DVB has standardized the scrambling algorithm for scrambling of channels (DVB-CSA) using CW, algorithms used for ECM/ EMM encryption are not standardized. Thus STBs having different CAS client cannot descramble the services. Currently, most of the CAS manufacturers are using DVB-CSA2 standard for scrambling of TS.

b) **Different Operating Systems/Middleware and other Drivers:** Operating System (OS) controls the various hardware modules of the STB and allows STB to execute different functions. To make the operation of STB user friendly and to simplify the search of TV channels, DVB specifies Service information (SI) tables. One such table is Event Information Table (EIT). The EIT contains the planned starting and stopping time of all TV programmes in form of Electronic Programme Guide (EPG). DVB has provided flexibility in the structure of EIT and allows any amount of additional information to be transmitted in EIT. Due to this flexibility, different service providers carry data in the EIT differently making non interoperability of EIT data. The Middleware of the STB helps in displaying the data contained in the EIT. There is no standard operating system/ middleware for STBs making the STBs non-interoperable. Besides this, the STB has a “loader” to enable DPOs to upgrade “resident applications” or download

"OS patches" to the STB. However presently, several mechanisms have been implemented in STBs hardware and software that ensure that only applications approved by CAS manufacturer are executed.

c) **Different Modulation Standards:** The signals are modulated before transmission. In cable TV, the signal is modulated using DVB-C standards whereas the signal is modulated using DVB-S standards 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 in the STB. Further, efficient versions namely DVB-C2 and DVB-S2 have been deployed by some 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 modulation standards.

d) **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. In the DTH sector both MPEG-2 and MPEG-4 deployment exists. While the MPEG4 standard is backward compatible, MPEG2 standard is not forward compatible. Therefore, MPEG2 compliant STBs cannot work in the MPEG4 networks.

3. As can be concluded from the above that the present eco system of STB is extremely rigid. There exists an end-to-end verticals of STB Manufacturer, Chip designer, CAS manufacturer, middleware, and DPO. Effectively, these results in STB being specific to the combination of DPO, CAS provider and STB manufacturer resulting into technical non-interoperable STBs.

C-DOT FRAMEWORK AND FEATURE REQUIREMENTS FOR THE ECOSYSTEM ENTITIES TOWARDS IMPLEMENTATION OF STB INTEROPERABILITY

Submitted to

The Telecom Regulatory Authority of India
TRAI, India

Version 3.0: Released on: August 2017

CENTRE FOR DEVELOPMENT OF TELEMATICS
MANDI ROAD, MEHRAULI, NEW DELHI 110030, INDIA
ELECTRONICS CITY (PHASE I), HOSUR ROAD, BANGALORE
560100, INDIA

Preface

This document gives a description of the C-DOT framework for Interoperable Set-top-box (STB) and the technical requirements for the Ecosystem entities towards implementation of the framework.

Acronyms

C-DOT : Centre for Development of Telematics

TRAI : Telecom Regulatory Authority of India

STB : Set-top-box

DTH : Direct-To-Home

CAS : Conditional Access system

SC : Smart Card

OS : Operating System

OTA : Over The Air

TS : Transport Stream

OTP : One Time Password

CAM : Conditional Access Module

1. BACKGROUND AND INTRODUCTION:

The digitization of cable TV network has led to huge deployment of STBs (Set Top Box). The market is expanding with nationwide adoption. India has large number of Direct-To-Home (DTH) subscribers. There are many MSOs (few thousands) and around 6/7 DTH operators in the country. IPTV penetration is expected to increase in future. Due to various technical, implementation and market driven reasons, presently the STB is tied to the service provider (operator). That is, the same STB cannot be used interchangeably across the service providers within a given segment (in case of MSOs and as well as DTH/IPTV operators). This vertical market structure has disadvantages for end users and also a major hindrance to technological innovation and industrial growth in this segment. C-DOT is working as Knowledge partner to TRAI towards developing a framework for STB interoperability.

This document gives the architectural details of C-DOT interoperable STB framework. It also details out the feature requirements of various ecosystem entities those need to be satisfied towards successful implementation of the interoperable STB framework.

In order to achieve interoperability of STB in an implementation scenario where multiple entities are involved, it is mandatorily required to evolve/formulate the corresponding specifications (in line with the architectural scheme detailed out in this document) and those specifications to be adhered to, by all the entities. In this context, it is pertinent to mention that these new specifications (to be formulated), will be an overlay on the existing international specifications and standards already being used in this technology segment.

2. TECHNICAL OBJECTIVES OF STB INTEROPERABILITY

The primary objective of STB interoperability is that the same STB shall be able to receive and decode/display signals from multiple operators. This implies that the STBs can be manufactured independent of any specific operator and CAS and can be used for receiving & viewing channels/programs from any operator in the field.

This also means that the basic EPG shall be working across multiple operators. There shall be a mechanism where operator specific middleware implementation variations can be programmatically read and adapted in STB. Also, it shall be possible to implement applications such as EPG and paves the way towards many other innovative apps in an open framework in order to offer sophisticated value added services and user experiences to the end users without STB being locked to a specific operator. The interoperable STB framework is discussed in details in the following chapters of this document.

3. STB INTEROPERABILITY: CORE TECHNICAL ISSUES

Before the interoperable STB framework is discussed, it is extremely important to analyze the core technical issues involved towards achieving STB interoperability.

- Conditional Access System (CAS), is by definition, proprietary. In many present day implementations, it is tightly coupled to STB hardware (in SoC), although there is no such mandatory provision mentioned in the prevailing standards.

- CAM is not cost effective. CAM is functionally almost as much as the STB itself. CAM based interoperability could not see market penetration due to different techno commercial reasons. The factors remain unchanged even for CI + 2.0 as well.

- Flexibility in prevailing standards and in some cases, non-adherence to the standard/recommendations during implementation, is major hurdle towards interoperability of STB specifically w.r.t. middleware.

- At present, the EPGs (Electronic Programming Guide) are non- interoperable due to above mentioned reason of flexibility and at times, non-adherence.

4. C-DOT FRAMEWORK FOR INTEROPERABLE STB

The following are the underlying fundamental principles of C-DOT framework for Interoperable STB:

- Use of a centralized TA (Trusted Authority) to allocate certificates / security codes to operators and STB manufacturers.
- Change of Operators with the change of operator specific smart cards using the same Interoperable STB: like mobile SIM cards in GSM handsets.
- This is an overlay on existing standards (DVB-C, DVB-S/S2),ISO 7816, ISO 13818, ETSI TS 101 211 etc
- Follows Kerckhoff's principle of cryptography [Contrary to "Security Through obscurity"].
- Industry standard cryptographic algorithms are being used in this framework to ensure security and ease of implementation.
- Operator specific Middleware adaptations in STB.
- The concepts of separable security and managed configurability in STB are being used in this framework.

The following are the ecosystem entities involved in the C-DOT framework for interoperable STB, many of these entities are very much prevalent in today's existing ecosystem as well. These entities are shown in the Fig. 1. It is pertinent to mention here that these are functional entities and at times two or more of these functions may be offered by a single physical entity/organization.

Trusted Authority (TA) is a new entity in the interoperable STB framework.

The entities on the right hand side in the Fig 1. are needed towards harmonious implementation and smooth proliferation of system elements (both Headend and STB) adhering to the framework in the network. All the equipment / sub-systems (both Headend & STB/Smart Card) are required to be certified by the certifying agency before deploying these in the network confirming the compliance to interoperability specifications.

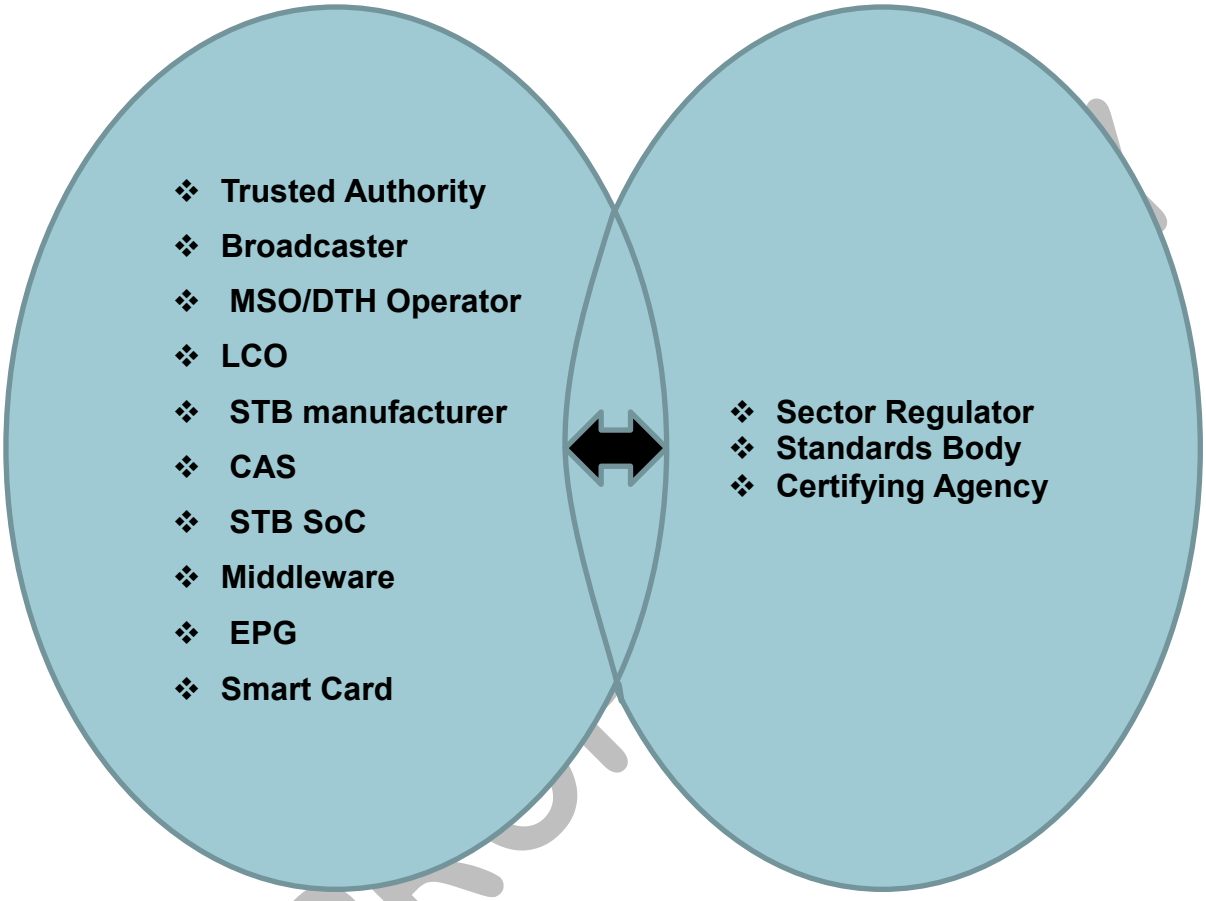


Fig 1. Stakeholders List

5. Architectural details of Interoperable Framework

C-DOT framework is based on operator specific detachable smart card approach. The exponential increase in the smart card processing power, security features & memory capacity (in Smart Card) and decreasing price gives an impetus to the concept of performing Conditional Access (CA) functions totally in Smart Card and also profiling the STB through the Smart Cards as per the service provider specific requirements towards interoperability. Smart cards (& on the TS/air) are embedded with greater operator specific intelligence/logic. For attaining interoperability, one obvious approach is to standardize all interfaces/functions, but such blanket

standardization has its own pitfalls. So far as conditional access is concerned, any blanket standardization is not desirable; however the underlying algorithms used in the interoperable framework are industry standard algorithms. The scheme proposed here mainly focuses on the downloading of profiling data from smart card and also over the air (through TS) to the STB and pushing CAS implementation entirely from STB to Smart Card. The STB shall have limited configurable features to support the operator specific requirements. The STB is not to be tied to any specific service operator and the same time cannot be fully generic configurable platform with the superset capabilities and the total software configurability, given the constrains of customer premise equipment. The STB is to be designed and manufactured (hardware and software) as per the interoperable specifications. Aspects pertaining to Headend elements are also considered as per the interoperable specifications satisfying the framework requirements. The profiling requirements in STB shall be such that the profiling data/functionality is minimal.

In this framework, the STB is configured according to the given context / operating environment of the operator/CAS by the intelligent Smart cards so that the required CA messages can be filtered in STB and sent to the Smart Card for further processing. The content security is of paramount importance in the framework. The security aspects specific to operator/CAS are processed in the detachable Smart Card. A lightweight communication protocol between STB and Smart Card with setup messages, information transfer messages, termination etc. is part of the framework. Bi-directional authentication scheme, secure channel establishment, a universal filter design for extracting the conditional access messages from the MPEG 2 transport streams for different service providers are also part of the framework. So the secure communication between the STB and Smart Card is formulated in the framework to enable interoperability of STB. The international standards (DVB, MPEG, ISO etc.) prevailing in the STB segment are to be adhered to along with some specific recommendations to achieve interoperability of middleware. Thus, the interoperable STB along with corresponding service provider's Smart Card is designed for receiving services from any service provider, in this framework.

5.1 Main Architectural Features

Interoperable STB broad architecture, functional blocks and Trusted Authority are shown in Figure 5, 2 and 3 respectively. The architectural details of the framework are as follows:

- Use of a Nodal agency (Trusted Authority) to issue authentication codes to both STB manufacturers and operators.
- Each operator will have their own smart cards that will inter-work with the interoperable STB.
- A light weight but highly secure layer between STB and Smart Card (SC) by using advanced cryptographic system suitable to interoperable STB context. Industry standard algorithms such as AES and RSA are used.
- Identification of operator configurable blocks in STB; configuration through smart card/over the air.
- Adaptation of industry standard algorithms with time variant dynamic session key generation to achieve high security.
- Mobile OTP based security augmentation (at the installation time, on a periodic basis and trigger based).
- Operator specific part of CAS in the smart card [ECM, EMM decryption etc.] retained unaltered leaving enough space for innovation by the CAS vendors.
- Operator specific Middleware adaptations in STB at the installation time.
- EPG is envisaged to be a STB feature. This is in line with mobile segment where a basic low end mobile will give only a very minimal UI where as a high end mobile when connected to the same network will give richer UI. However there is provision for down loading the operator specific machine readable EPG through OTA.
- Secure boot is an essential feature and is also taken into considerations in this framework. In present day implementation, secure boot is CAS specific; in the interoperable framework, the secure boot is achieved using manufacturer's signature which is independent of any CAS. Similarly for OTA also manufacturer's signature is used along with Operators credentials for verifications.

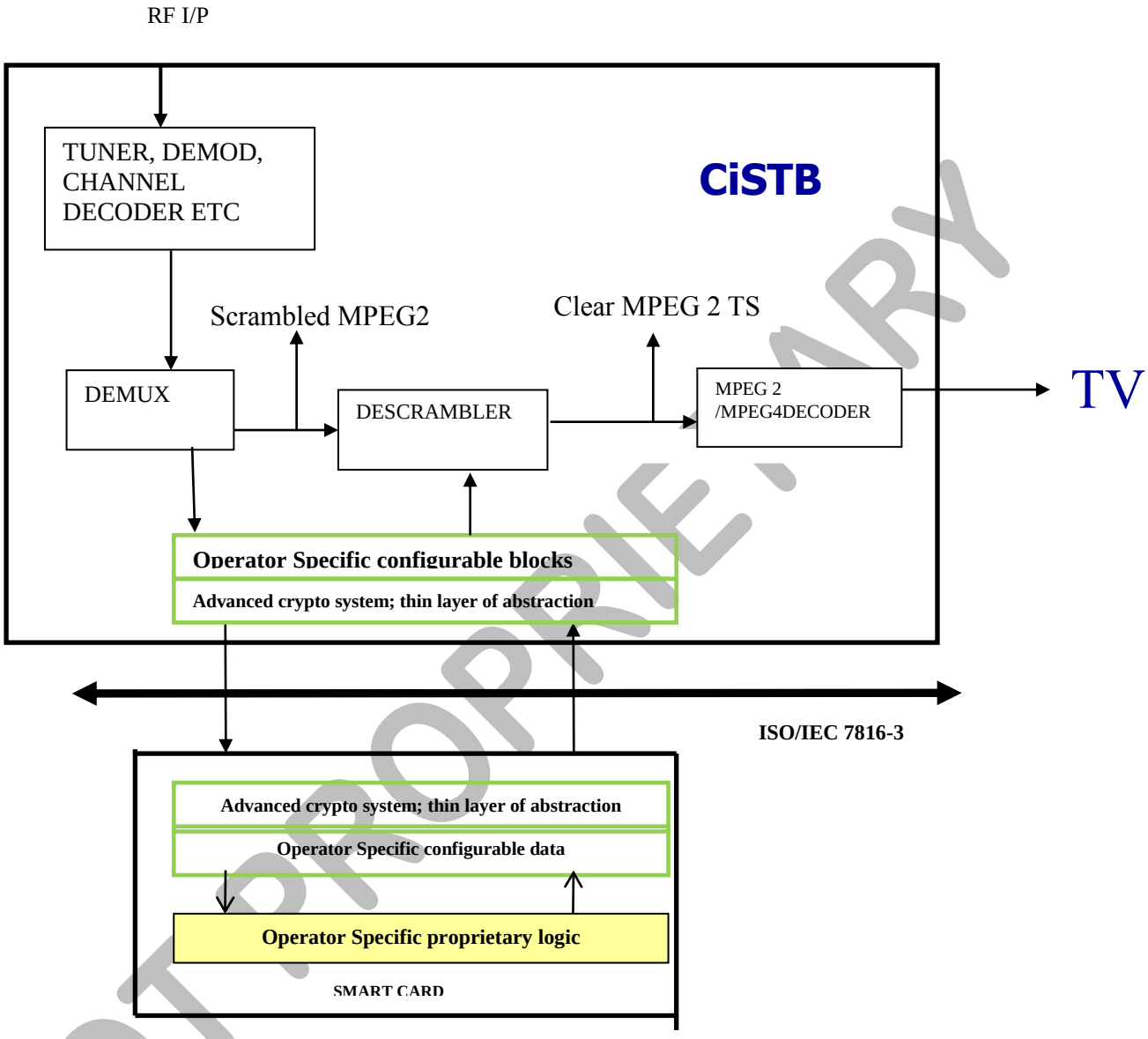


Fig 2: Smart Card based interoperable STB

Modules specific to (tied to) a particular CAS(As per the Transmit side CA). Proprietary to Operator / CAS vendor.

"Advanced Crypto system (Thin layer of abstraction)" and "Operator Specific configurable data" are part of the evolved interoperable framework to be adhered to by all interoperable STBs and User Smart Cards issued by the operators. This is an overlay on existing international standards. Operator specific configurable blocks in STB consist of CA (Conditional Access) Filter and other Middleware specific modules.

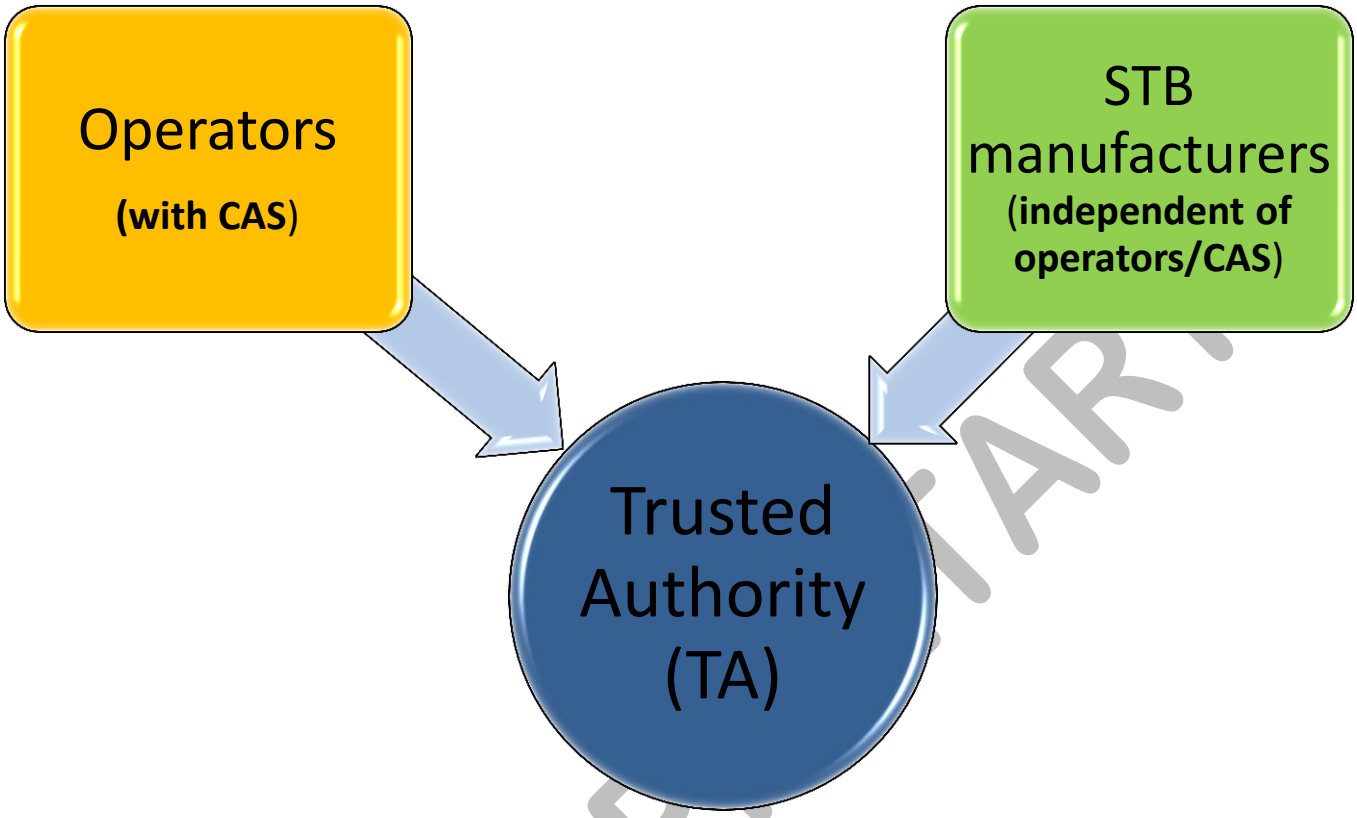


Fig 3: TRUSTED AUTHORITY AND OTHER ENTITIES

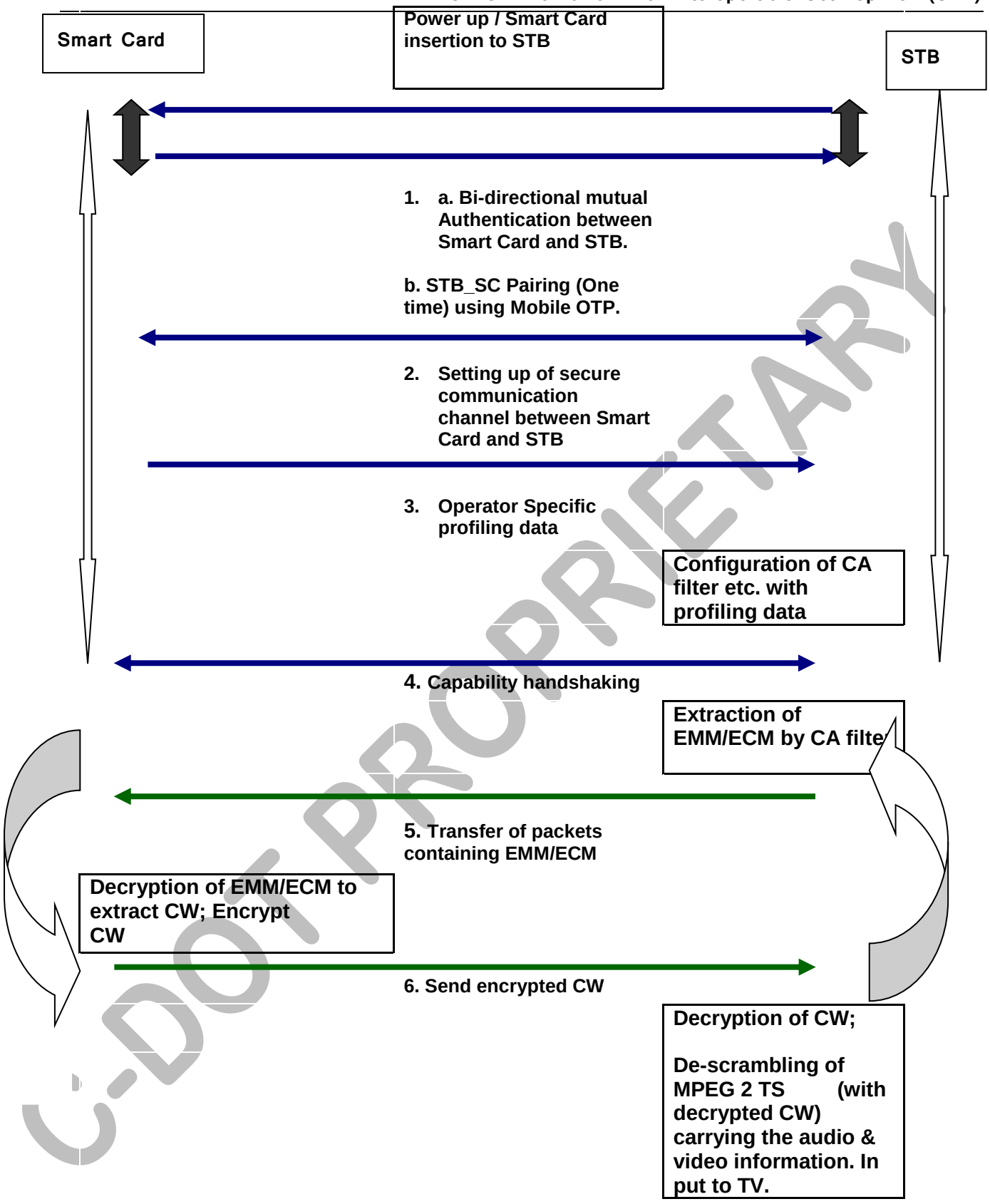


Fig 4: High level Message Transfer Sequence between Smart Card and STB

5.2 INTEROPERABLE STB ARCHITECTURE

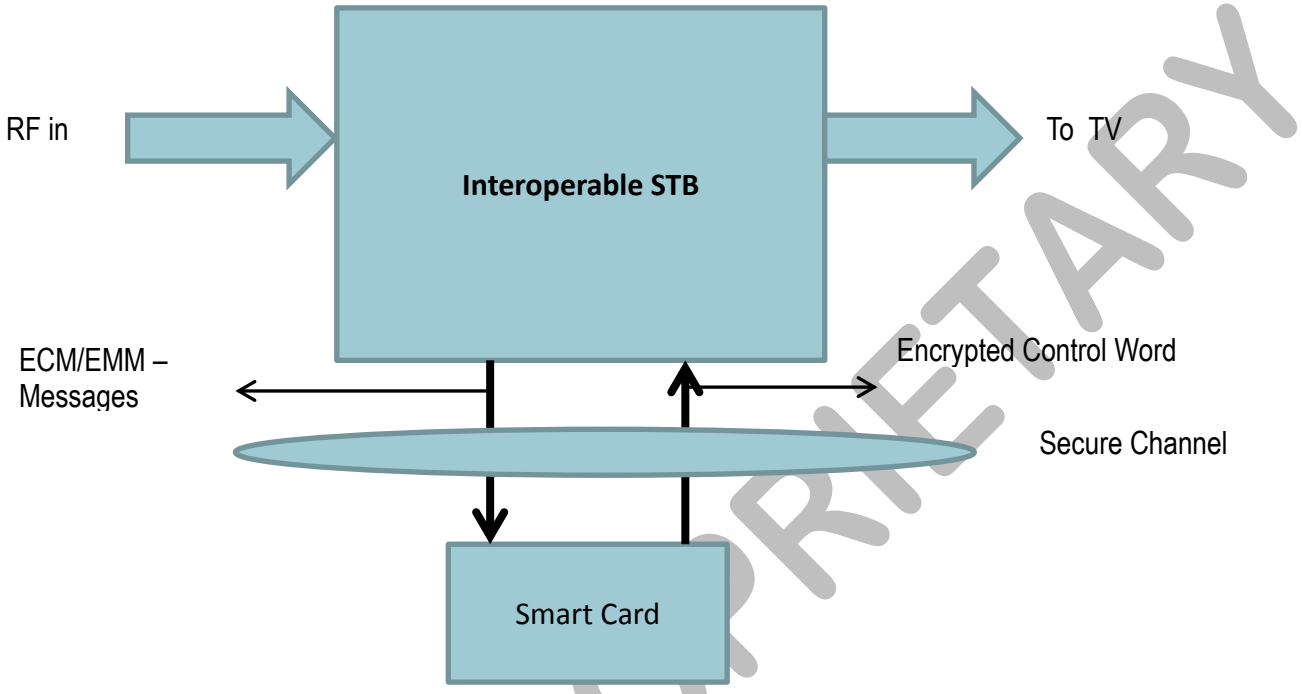


Fig 5: High Level diagram of Interoperable STB

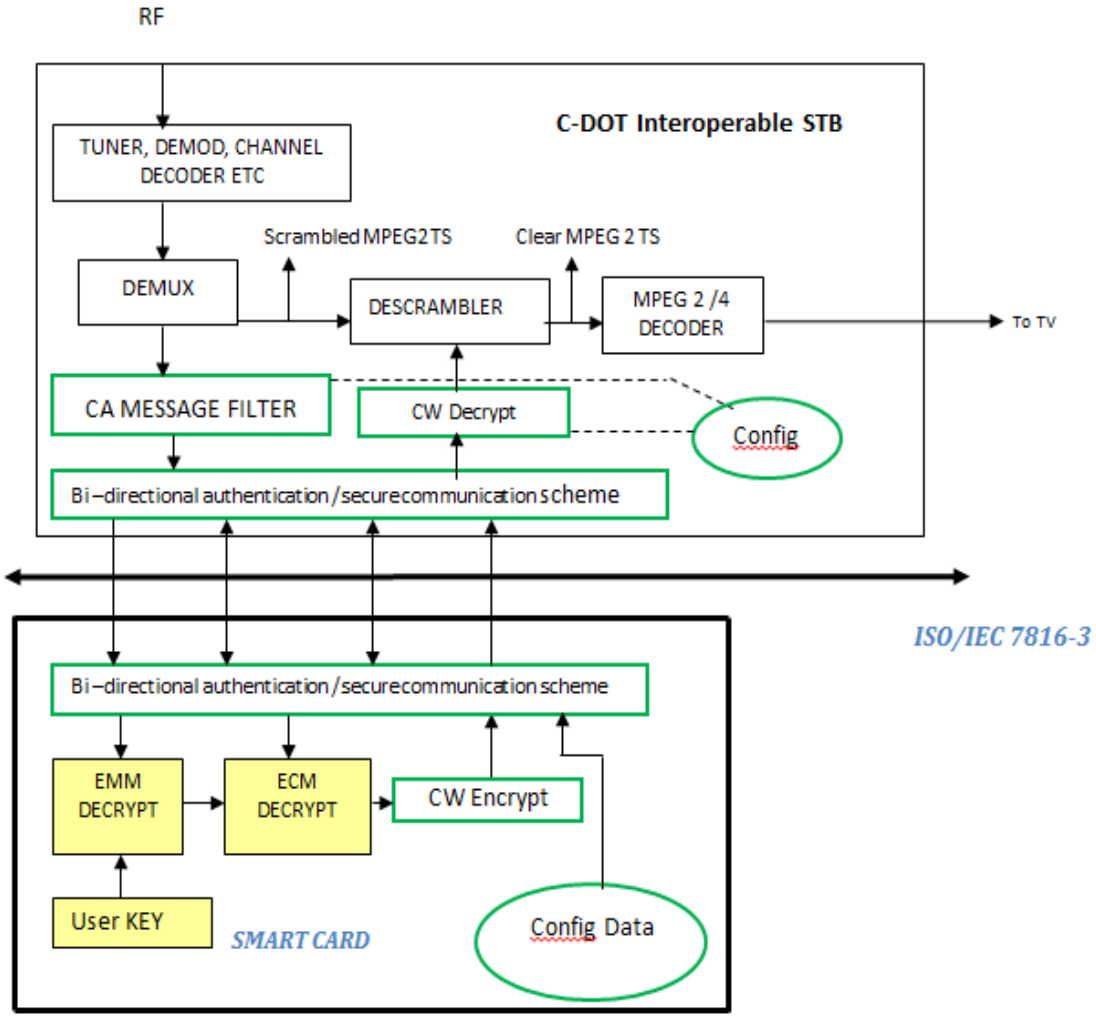
High level architecture diagram for interoperable STB is shown in Figure 5. Interoperable STB functional block diagram is shown in the figure 2. The internal blocks are shown in Fig 6.

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. STB processes the control information consisting of different PSI/SI tables to perform further decoding of the TS. If the programme is not scrambled the STB decompresses the programme and transform the digital signal into a regular TV signal, data stream, or other type of flow according to the kind of data being

broadcast. If the programme is scrambled, the STB extracts the entitlement control message (ECM) and relevant entitlement management message (EMM) from the MPEG-2 transport stream and sends to the smart card. The smart card decrypts EMM and ECM and sends the decrypted key (CW) which descrambles the actual content through secure channel to STB. The CAS specific proprietary modules are available / embedded only in the Smart Card and not on STB. STBs are CAS/operator agnostic at the design and manufacturing stage as part of interoperable requirement. Also there are some configurable blocks in STB, those are configured as per the operator/CAS on installation/run time. The Smart Card interface is compliant to ISO/IEC 7816-1,2,3. A layer of abstraction for interoperability is defined on top of ISO/IEC 7816-1,2,3.

ISO/IEC 7816-1: Gives the physical Characteristics of the cards.
ISO/IEC 7816-2: Gives dimension and location of the cards.
ISO/IEC 7816-3: Gives electrical interface and transmission protocol.

APDU commands of ISO/IEC 7816-4 are also used.



"Bi-directional authentication / secure communication scheme" and "configurable data/blocks" are part of the evolved interoperable framework to be adhered to by all interoperable STBs and User Smart Cards issued by the operators. This is an overlay on existing international standards. Operator specific configurable blocks in STB consist of CA (Conditional Access) Filter and other Middleware specific modules.

Modules specific to (tied to) a particular CAS(As per the Transmit side CA). Proprietary to Operator / CAS vendor.

Fig. 6 : Internal Blocks of Interoperable STB

The generic functional blocks in interoperable STB are:

- RF tuners, demodulators, FEC decoders.
- Demultiplexer
- Controller.
- Descrambler
- Media Decoder (MPEG2/MPEG4)
- Operator Specific Configurable Block (Configurable CA / Message filter)
- Advance crypto module for STB - Smart Card interface.

The generic functional blocks in Smart Card are:

- Advance crypto module for STB - Smart Card interface
- Operator Specific Configurable Data
- Operator specific proprietary logic

As part of the interoperable framework, the following two functional blocks are defined:

i. Advance crypto module for STB - Smart Card interface (on top of ISO 7816-1,2,3)
ii. Operator Specific Configurable Data/module

All other blocks in interoperable STB are as per existing open standards and in smart card the ECM/EMM decryption is operator/CAS specific.

5.3 WORK FLOW DETAIL

Work flow detail gives the steps involved towards working of interoperable STB at preparation phase and at runtime. As per the framework requirements, an appropriate Trusted Authority (TA) is assumed to be in place.

1. Preparation Phase:
    i. Registration of STB Manufacturers and Operators with TA.

ii. TA allocates certificates /Key Pair to STB Manufacturers and Operators.

iii. STB Manufacturer generates key pairs and certificates for individual STBs and stores the private key and certificates in the secure memory of each STB. STB manufacturer works as secondary TA.

iv. Operator generates key pairs and certificates for individual SC and stores the private key and certificates in the secure memory of each SC. Operator works as secondary TA.

2. Runtime :

i. Smart Card is inserted in the STB and is powered up.

ii. Bi-directional authentication takes place between STB and SC.

iii. After successful bi-directional authentication, there will be OTP based pairing procedure (for the first time or Operator initiated).

iv. Configuration of STB (one time and as and when needed) as per operator.

v. Control messages (ECM/EMM) are filtered and sent to SC

vi. SC decrypts the CWfrom ECM/EMM and re-encrypts the CW.

vii. The re-encrypted CW is sent from SC to STB.

viii. STB decrypts the re-encrypted CW for content descrambling.

5.4 FUNCTIONAL MODULES REQUIRED TOWARDS ATTAINING INTEROPERABILITY

a. Bi-directional authentication scheme between STB and Smart Card.

b. OTP based security module through mobile network.

c. STB-Smart Card-Registered Mobile Number Pairing scheme

d. Runtime Safe Channel Setup between Smart Card and STB

e. Operator specific profiling data

f. Configurable CA filter

The above mentioned functional blocks are detailed below.

a. Bi-directional Mutual authentication scheme between STB and Smart Card:

The bi-directional mutual authentication algorithm between STB and Smart Cards is based on the following mechanism:
Bi-directional mutual authentication between STB and Smart Card is a very important step. Every time the STB is powered on or Smart Card is inserted in STB, this step is initiated. In an interoperable regime, the STB is considered a retail item and is manufactured independent of any specific operator / CAS; only operator & user specific smart card is issued by the operator. Here as the STB and Smart card are independently manufactured, it is important that these two modules authenticate each other before they start sharing secure information. This ensures that STB is communicating with a genuine Smart Card and ensures the Smart Card that it is communicating with a genuine STB. In this scheme of bi-directional authentication, no permanent key of STB is pre stored in Smart Card and no permanent key of Smart Card is pre-stored in STB. The bi-directional authentication takes place based on TA as root of trust and dynamic challenge response mechanism.

The following are the details of Bi-directional authentication.

- Based on TA (Trusted Authority) certificate/authentication code based approach.
- Challenge Response mechanism between STB and Smart Card.
- Uses standard Asymmetric and symmetric key cryptographic algorithms.
- Derivation of Temporary session Keys.
- Secure encryption schemes suitable for smart card processing capabilities.
- Mechanism to overcome McCormac Hack, Man-in-Middle attack etc.

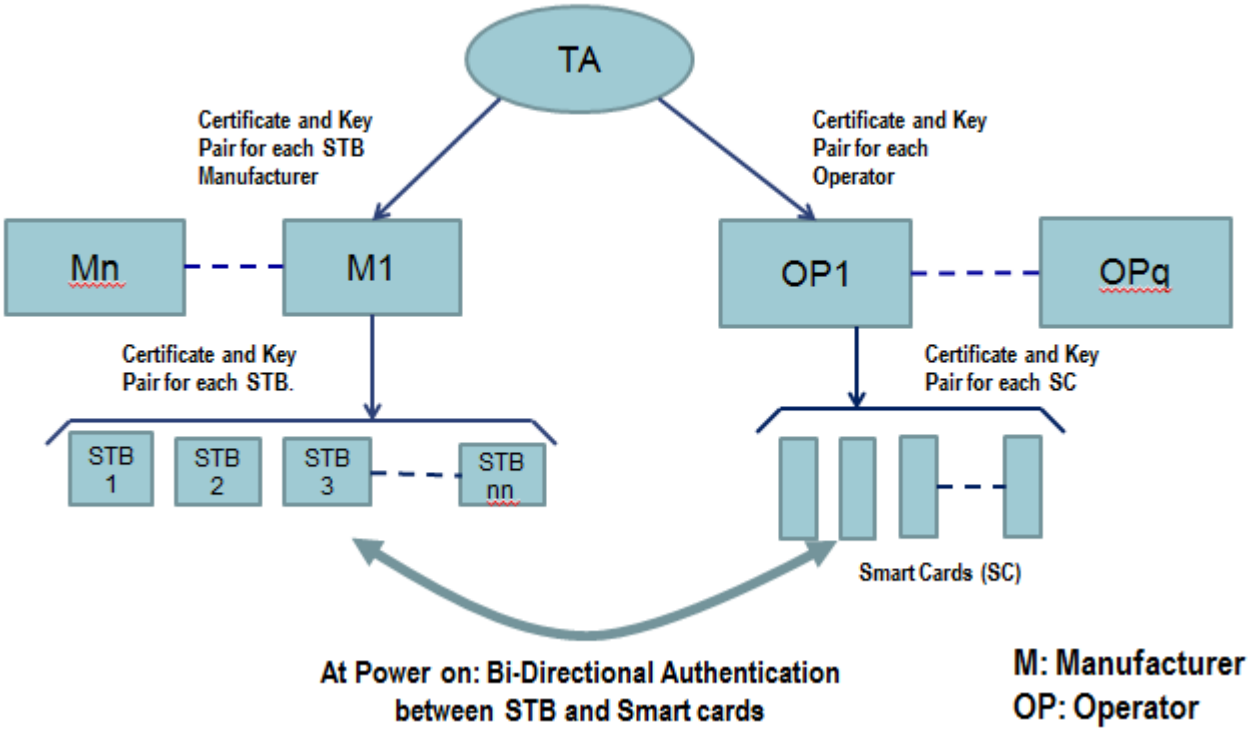


Fig 7: Bi-directional authentication

Trusted Authority (TA) is a National Entity and serves as root of trust. TA allocates Public /Private Key pairs to Operators (CAS) and to STB manufacturers.

Operators intern generate Public/Private Key pairs for all its users/subscribers/smart cards. Private Key of the smart card is stored in the secure memory of the smart card. Similarly, manufacturers generate Public/Private Key pairs for all the STBs it manufactures (as shown in Fig. 7). Private key is stored in the secure memory of STB. When Smart Card is inserted into the STB, the STB authenticates the Smart Card and also Smart Card authenticates the STB. The bidirectional authentication takes place considering TA's public key / information as the common/root trust. During successful bidirectional authentication between STB and Smart Card, a random session key is generated in Smart Card and securely shared with STB using mainly asymmetric key cryptographic schemes. After successful bi-directional authentication, this dynamic session key is used to encrypt the CW in the Smart Card while transmitting the CW to the STB, for the duration of the session (session

duration can be fixed by the operators – typically around 30 minutes). STB decrypts the CW with the already securely shared session key and use the decrypted CW to descramble the scrambled program. After the expiry of the session, again a new session key gets generated, securely shared between STB and Smart Card and is used.

Bidirectional Authentication protocol

Protocol

This protocol has two phases: a preparation phase and a communication phase. These two phases are described respectively as follows.

The Preparation Phase

The preparation phase involves the trusted authority (TA), which has a pair of public/private keys **(pk_{TA},sk_{TA})**, STB manufacturer(SM), and MSO/DTH operator (OP) which also functions as secondary trusted authority.

1) TA generates a unique identification string I_{SM}, a pair of public/private keys **(pk_{SM},sk_{SM})**, and the corresponding public key certificate $C_{TA}(I_{SM}) = I_{SM}, pk_{SM}, sig_A(I_{SM}, pk_{SM})$ for each STB manufacturer, where $sig_{TA}(I_{SM}, pk_{SM})$ denotes TA's signature on the message (I_{SM}, pk_{SM}) with private key sk_{TA}. Then TA safely delivers pk_{TA} and sk_{SM}, $C_{TA}(I_{SM})$ to the STB manufacturer by a trust carrier or through a secure channel between TA and STB manufacturer.

2) The SM generates a unique identification string I_{STB}, a pair of public/private keys (pk_{STB}, sk_{STB}), corresponding public key certificate $C_{SM}(I_{STB}) = I_{STB}, pk_{STB}, sig_{SM}(I_{STB}, pk_{STB})$ for each STB, where $sig_{SM}(I_{STB}, pk_{STB})$ denotes SM's signature on the message (I_{STB}, pk_{STB}) with private key sk_{SM}.Then SM stores $pk_{TA}, C_{TA}(I_{SM}), C_{SM}(I_{STB}), sk_{STB}$ into the secure memory of each STB at the stage of producing STB.

SM also stores details of symmetric key algorithm E_k (·), public key algorithm E_{pk} (·), and hash algorithm h(·) to be used in communication phase in each STB.

Where, $\mathbf{sig_X(M) = E_{PKx}[h(M)]}$

And following are the recommended algorithms to be used where required:

E_{pk}(.) : RSA-2048

E_k(.): AES-128

h(.): SHA-256

3) The TA generates a unique identification string I_O, pair of public/private keys **(pk_{OP}, sk_{OP})**, and a public-key certificate $\mathbf{C_{TA}(I_{OP}) = I_{OP}, pk_{OP}, sig_{TA}(I_{OP}, pk_{OP})}$ for each OP. The TA safely delivers the set of messages $\mathbf{pk_{TA}}$, $\mathbf{C_{TA}(I_{OP})}$, $\mathbf{sk_{OP}}$ to each OP.

4) The OP generates a unique identification string $\mathbf{I_{SC}}$, a pair of public/private keys **(pk_{SC}, sk_{SC})**, corresponding public key certificate $\mathbf{C_{OP}(I_{SC})}$ = $\mathbf{I_{SC}}$, $\mathbf{pk_{SC}, sig_{OP}(I_{SC}}$, $\mathbf{pk_{SC})}$ for each Smartcard (SC), where$\mathbf{sig_{OP}(I_{SC}}$, $\mathbf{pk_{SC})}$ denotes OP's signature on the message $\mathbf{(I_{SC}}$, $\mathbf{pk_{SC})}$ with private key $\mathbf{sk_{OP}}$.Then OP stores $\mathbf{pk_{TA}, C_{TA}(I_{OP}), C_{OP}(I_{SC}), sk_{SC}}$ into the secure memory of each SC.

OP also stores details of symmetric key algorithm E_k (·), public key algorithm E_{pk} (·), and hash algorithm h(·) to be used in communication phase in each SC.

The Communication Phase (Run Time)

In this phase, SC is inserted in STB or each time STB is powered up with SC inserted, both STB and SC perform the following operations/steps:

1) STB sends the SM's certificate $\mathbf{C_{TA}(I_{SM})}$ to SC.
2) SC verifies the certificate $\mathbf{C_{TA}(I_{SM})}$ using the TA's public key $\mathbf{pk_{TA}}$. If the result of the verification is positive, SC replies with success status bytes (e.g. 90 00) to STB and stores $\mathbf{I_{SM}}$,$\mathbf{pk_{SM}}$, otherwise sends the error status to the STB,

discards $\mathbf{I_{SM}}$, $\mathbf{pk_{SM}}$and resets its state to step 1 (now it will expect STB to send SM's certificate again).

3) STB sends its certificate $\mathbf{C_{SM}(I_{STB})}$ to SC.
4) SC verifies the certificate $\mathbf{C_{SM}(I_{STB})}$ using the SM's public key $\mathbf{pk_{SM}}$. If the result of the verification is positive, SC replies with success status bytes (e.g. 90 00) to STB and stores $\mathbf{I_{STB}}$,$\mathbf{pk_{STB}}$, otherwise sends the error status to the STB, discards $\mathbf{I_{STB}}$,$\mathbf{pk_{STB}}$ and resets its state to step 1.
5) STB asks SC for the OP's certificate $\mathbf{C_{TA}(I_{OP})}$. SC sends it to the STB in reply.
6) STB verifies the certificate $\mathbf{C_{TA}(I_{OP})}$ using the TA's public key $\mathbf{pk_{TA}}$. If the result of the verification is positive, STB stores $\mathbf{I_{OP}}$, $\mathbf{pk_{OP}}$, otherwise discards them and stops the communication with SC and waits for SC removal. When SC is removed and same/new SC is inserted, STB resets its state to step 1.
7) STB asks SC for the SC's certificate $\mathbf{C_{OP}(I_{SC})}$. SC sends it to the STB in reply.
8) STB verifies the certificate $\mathbf{C_{OP}(I_{SC})}$ using the OP's public key $\mathbf{pk_{OP}}$. If the result of the verification is positive, STB stores $\mathbf{I_{SC}}$, $\mathbf{pk_{SC}}$, otherwise discards them and stops the communication with SC and waits for SC removal. When SC is removed and same/new SC is inserted, STB resets its state to step 1.
9) STB generates a random nonce $\mathbf{r_1}$,encrypts it with the SC's public key $\mathbf{pk_{SC}}$and sends it to the SC.
10) SC decrypts received message using its private key $\mathbf{sk_{SC}}$to get $\mathbf{r_1}$. Then SC generates a random session key **K** and a random nonce $\mathbf{r_2}$
11) SC encrypts session key **K**with $\mathbf{pk_{STB}}$ and nonce $\mathbf{r_1}$, $\mathbf{r_2}$ with session key **K**. And send both encrypted messages to STB.
12) STB decrypts $\mathbf{E_{PKstb}[K]}$ using $\mathbf{sk_{STB}}$and $\mathbf{E_K[r_1,r_2]}$ using **K**.. STB matches the decrypted value of $\mathbf{r_1}$ with original value of $\mathbf{r_1}$.If both values are matched correctly, then SC is authenticated by STB successfully. Otherwise, STB stops the communication with SC and waits for SC removal. When SC is removed and same/new SC is inserted, STB resets its state to step 1.
13) STB then encrypts $\mathbf{r_2}$ using K andsends it to SC. SC decrypts it and checks if this value of $\mathbf{r_2}$ matches with the original value of $\mathbf{r_2}$. If they match, then STB is authenticated by SC successfully. Otherwise, SC resets its state to step 1.

Storage guidelines for security:

STB data	Smartcard data
$C_{TA}(I_{SM})$: ROM*	$C_{TA}(I_O)$: ROM
$C_{SM}(I_{STB})$: ROM	$C_O(I_{SC})$: ROM
pk_{TA} : ROM	pk_{TA} : ROM
sk_{STB} : Secure ROM**	sk_{SC} : Secure ROM
Pk_O : RAM	Pk_{SM} : RAM
pk_{SC} : RAM	pk_{STB} : RAM
r_1 : RAM	r_1 : RAM
r_2 : RAM	r_2 : RAM
K : Hardware-configured***	K : Hardware-configured

Note:

*: This data needs to be read-only and can be read by any software or hardware module.

**: This data needs to be read-only and accessible to only secure modules which don't expose data outside the SOC. Such data must be directly given as input to the necessary hardware/secure processor and should not be accessible to any other software or hardware module outside SOC.

***: Session key K when decrypted using crypto hardware must be fed directly to symmetric Cipher hardware, without exposing it outside SOC

b. OTP based security module through mobile network

The mobile OTP scheme is used on top of (in addition to) bidirectional authentication scheme and other mechanisms as described in this framework document. Although there is various advanced security mechanisms inherently available in the state of the art Smart cards and are being further enhanced from time to time as a natural evolution of technology, the mobile OTP mechanism adds further level of security on the top of these mechanisms. Mobile OTP

schemes are very much prevalent in providing/enhancing security in Internet banking segments etc.; although the exact detail steps in the schemes are different, owing to some of the specific feature differences in the segments and use cases.

The following diagram (Fig. 8) shows the mobile OTP based security scheme:

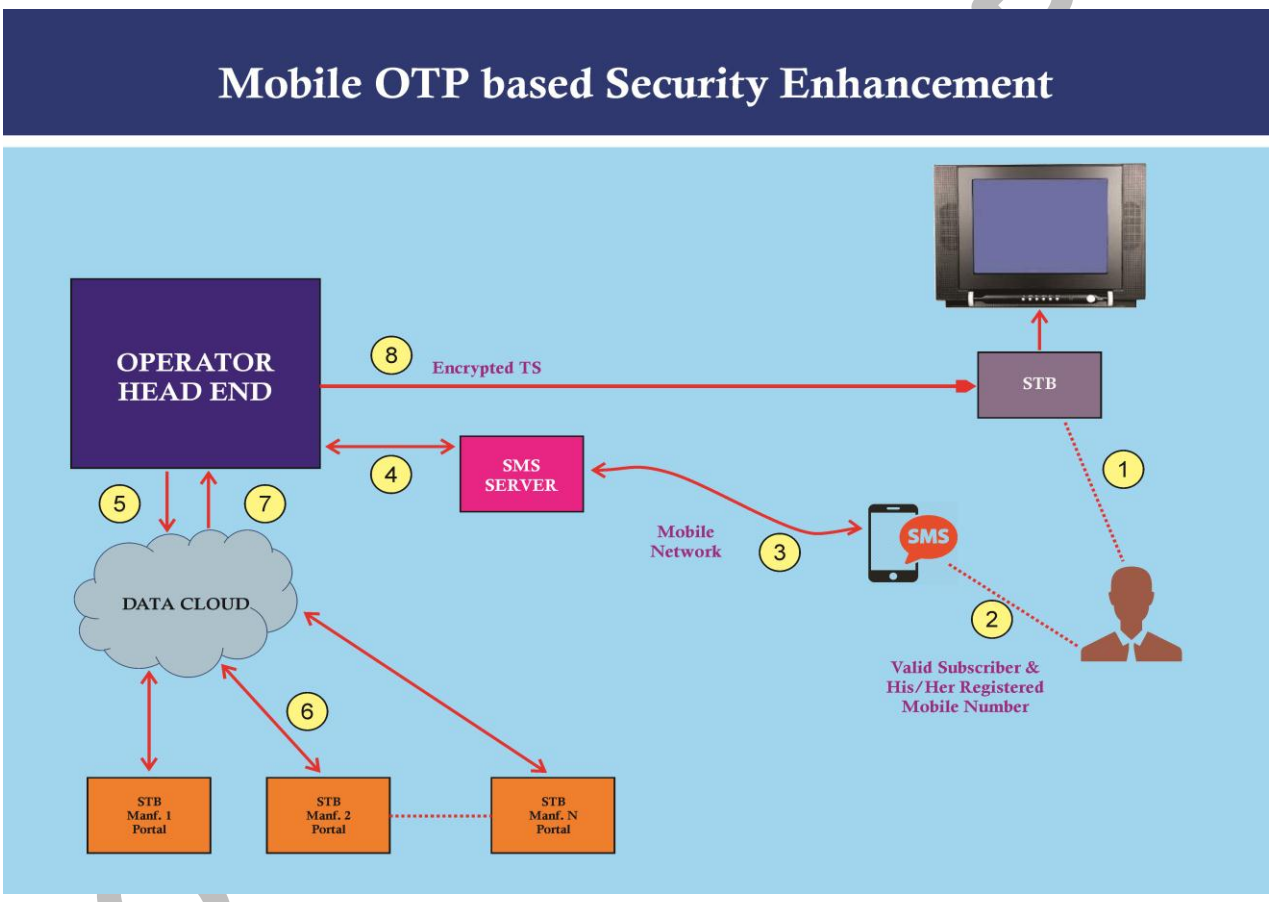


Fig 8: Mobile OTP Based Security Enhancements

Mobile OTP scheme:

User buys a subscription from an operator. Operator provides him/her a unique smart card (pre-configured with operator specific information). Along with that operator stores user's registered mobile number, customer id, Smart Card-id and other some other user specific information in its Headend database. A user buys

a STB from the retail outlet which is also compatible with OTP based registration process. This STB can be uniquely identified by a 64-bit STB-ID which comprises of STB's manufacturer ID also. STB_ID is same as I_{STB} as mentioned in Bi-directional authentication scheme (Section 'a').

When user inserts the smart card in this STB and powers it on, following process takes place between STB and smart card with involvement of user and the operator:

I. STB and smartcard undergo a mutual authentication process to securely share a session key. This session key is used to share any data between STB and smartcard.

II. STB asks for the registration process status to the smart card. Smart card sends it to STB. Now STB checks its internal flag of registration status as well as the one sent by smart card. If either of them is false, it will display a message for the User to complete the registration process. Message displayed by STB on TV contains SMS format to be sent to the operator along with the operator's number. For the first time registration using a new STB with user's smart card, user has to send STB-ID to the operator compulsorily. If same STB was used previously with the user's smart card for registration process, user can send only "RENEW" as the content of SMS instead of sending full STB-ID.

III. User reads the message on TV and he lands on the menu item specially designed to complete this procedure.

IV. User sends message to the operator as per the message displayed on TV along with the Smart Card id. For the first time when the STB is put on a new operator network, the registered mobile of the authorized installation/service person can also be use to send these information to the operator. However, the OTP (as detailed in the subsequent steps) is sent by the operator to the registered user's mobile number only.

V. The operator first checks whether mobile number and Smart Card id is registered in its database and then locates corresponding user. Operator will then check the number of requests received from the user recently and stops responding to requests from that user if it exceeds the predefined limit (This limit is kept to prohibit adversary to use any brute-force method for attacking STB's security by

sending repeated requests. This also helps operator to minimize server's load as well as EMM bandwidth due to repeated requests). If user sends STB-ID in the message, operator checks the manufacturer ID and gets corresponding STB's public key from manufacturer's portal (using access rights given by the manufacturer). Then operator will replace current with older STB-ID in its database. If user doesn't send STB-ID, STB-ID stored in database will be used for registration process. The operator generates an "N" digit random and unique OTP for the user and sends this OTP via SMS to the user. Operator also sends one trigger control message which enables smart card to accept OTP entered by user. Trigger control message is identified by STB using Table-id field.

VI. This Trigger message contains STB-ID, Hash of OTP and two level encryption of a new symmetric key (called as periodic key, PK), some filters for control messages along with validity of OTP, timestamp. First level of encryption is done by a temporary key TK formed using user key (UK) and OTP. Then it is re-encrypted using the STB's public key (PKs). The periodic key (PK) to be used by operator to encrypt all user specific control messages which are sent after the registration process.

The typical structure of trigger message to be sent by operator to STB is shown below. Trigger message requires two TS packets.

TS header	Zero byte	Table ID	Section syntax indicator	CA_length	STB-ID	Seq No=1	H(OTP)	$E_{PKs}[E_{TK}$[PK, filters, OTP validity, timestamp]]: Part 1	CRC
32 bits (4B)	8 bits (1B)	8 bits (1B)	16 bits (2B)		64 bits (8B)	8 bits (1B)	128 bits (16B)	1216 bits (151B)	32 bits (4B)
TS header	Zero byte	Table ID	Section syntax indicator	CA_length	STB-ID	Seq No=2	$E_{PKs}[E_{TK}$[PK, filters, OTP validity, timestamp]] : Part 2		CRC
32 bits (4B)	8 bits (1B)	8 bits (1B)	16 bits (2B)		64 bits (8B)	8 bits (1B)	832 bits (105B)		32 bits (4B)

As each TS packet size is limited to 188 bytes, hence for the purpose of sending this trigger message two TS packets are needed.

Here,

E_{pks}(.) : RSA-2048

E_{TK}(.): AES-128

h(.): SHA-256

VII. As soon as STB gets the Trigger message, it matches the STB-ID sent inside message with its STB-ID. If it matches, then it decrypts the encrypted part of the message with its private key and then sends decrypted Trigger message to the smart card. If STB-ID doesn't match, STB ignores that message.

VIII. Smart card gets the Trigger message and sends instructions to STB to accept OTP from user and waits for OTP from STB.

IX. STB sends the OTP entered by user to smartcard.

X. Smart card generates the hash of the OTP entered by user and verifies with the one received in the trigger message. If it matches then smart card first gets the temporary key (TK) by using UK and OTP (with same function as used by operator) and decrypts the encrypted part of the message using TK to get PK, control filters, validity of OTP and timestamp of the trigger message.

XI. Smart card stores this timestamp in its memory and uses it as reference to calculate elapsed time after registration process. This is used to keep check on the validity of registration process.

XII. If registration process is successful, then smart card sends registration status to the STB along with the validity of OTP, control filters and timestamp received in trigger message. STB displays message on the TV based on the status sent by smart card. STB also confirms whether the trigger message was received before storing validity of OTP and control filters in its memory. STB sends a fresh (random) pairing-id to smart card. Smart card stores it in a secure memory. Similarly smartcard also generates and sends a fresh (random) pairing-id to STB. STB stores it in its memory securely (This is

needed to avoid bypassing of pairing-id checking by STB). Also pairing-ids are separately encrypted and stored in STB and same way in SC. STB also keeps check on validity of registration process independently of smart card using time information received from operator.

XIII. If the registration process fails, STB displays the same on TV along with the reason of failure and asks user to start registration process again.

XIV. When STB is powered on next time after successful registration process, it gets registration process success status from smart card.

XV. If registration process status is true and matches STB's internal flag, STB asks the pairing-id from the smart card which was shared with it after the completion of last registration process. If this pairing-id matches with the pairing-id stored in STB, then STB starts sending control messages (ECMs and EMMs) to the smart card. Otherwise it asks user to complete registration process again. This confirms whether the same smart card was used with the current STB for registration process.

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.

XVII. User can be given a grace period of 2-3 days to complete this procedure again before expiration of previous key.

XVIII. 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.

XIX. If operator suspects any security breach in the network, it can initiate the registration process for any number of users after informing them about the same.

Data Storage in STB, smartcard and operator:

From the security point of view, following parameters should be kept secure in genuine STB and smartcard:

STB: STB-ID, Registration process status, Validity of OTP, pairing-id, sk_{STB}

Smartcard: Registration process status, STB-ID, Periodic key, user key, subscription data, Validity of OTP, pairing-id.

Operator (Headend): Validity of OTP, STB-ID, smartcard-id, registered mobile number, Periodic key (PK), User Key (UK).

Security Enhancements / advantages with mobile OTP based Scheme:

The mobile OTP algorithm minimizes the effect of cloning attacks significantly which is more prevalent these days, by having a reverse channel via registered mobile number. Since operators keep the subscriber information which include subscriber ID, address along with his mobile number, the registered mobile number can be used for enforcing authorized usage of his subscription.

Even if any adversary has a valid subscription, he should not be able to let multiple users use his subscription without paying for it to the operator. This can be ensured using an OTP verification process which has to be completed by every user periodically in order to keep his subscription running. Unauthorized users will not be able to complete OTP verification since they don't have registered mobile number with them. During OTP verification process, operator sends a fresh key which will be used to encrypt the subscriber's entitlement data for next period. So even if an adversary tries to skip OTP verification process somehow through modification of smart cards, he will not be able to decrypt his entitlement messages due to lack of key required for it. Consequently, he will not be able to access any unsubscribed service.

Also this algorithm adds multiple levels of security. So even if smart card is cloned, it cannot be used on any STB other than the authorized subscriber is using and vice versa. In other words, subscriber's STB, smart card and the registered mobile number are all tightly bound to each other and unauthorized usage of subscription is not possible if the user does not have access to even single entity out of these three.

c. STB – Smart Card – Registered Mobile Number pairing scheme.

- One Time registration of STB with operator using the user's registered mobile number.
- Mobile network based Pairing of STB – SC – Mobile No.
- STB duplication detection mechanism
- Protection against Smart Card cloning
- Dynamic updating of STB – SC – Mobile No list.

Each time the interoperable STB is installed in the new operators' network, the STB gets registered with the operator using the registered mobile number of the user. This dynamic pairing of STB with Smart Card and mobile number is useful towards secure service delivery of content to the user. The mechanism as explained in section 'b' above is used.

d. Runtime Safe (Secure) channel Setup between Smart Card and STB.

After the successful bi-directional mutual authentication (as shown in the Fig 4), the EMM/ECM is extracted by STB and sent to Smart card. 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.

The control word (CW) derived by the Smart card from the EMM/ECM and private data, shall not be sent as a clear data to STB. Otherwise CW can be tapped and used in many decoders / STBs to receive the pay TV signals. Similarly security sensitive information from STB to Smart card shall be sent through a safe channel. The dynamic session key securely shared between STB and Smart Card (as detailed in section 'a' above) is used as key to establish the secure channel between Smart Card and STB.

The safe channel between STB and SC (in both the direction) is ensured by two mechanisms:

- One time session key generation
- Encryption of EMM

So, in this scheme, the key used for encrypting CW in Smart Card is shared with STB using the mechanism as explained in section ‘a’ above. AES-128 is used to encrypt the CW while sending it from SC to STB. The session key can be regenerated and shared between SC and STB on a periodic basis. EMM is encrypted with user specific Periodic Key ‘PK’ as detailed in the section ‘b’ above.

e. Operator Specific profiling data

- The operator specific profiling data is stored in Smart card by the operator before it is issued to the subscribers/users. In this scheme, these profiling data is used by STB to attain interoperability as well as can help in enhancing the security of the system. The profiling data can be sent over the air as well. In this context it is important to mention that although there is a mechanism provided to use operator specific configuration data (through smart card and/or over the air), it is required that the Headend and STB adheres to the recommended ETSI specifications (as mentioned in section 6.c) and this configuration data is intended to be kept at minimum.

The profiling data used for the following purposes:

- These data can be used to configure the CA filter (of STB) so that the relevant CA messages along with private data can be sent to Smart card from STB.Some of the middleware related information are part of the profiling data. Existing capabilities of STB are verified and the mutually supported set of features are agreed upon those can be delivered by the operator using the specific STB are finalized and presented to the customer before the actual delivery of service. Support of type of compression techniques etc. can be decided. This feature is very useful for attaining total interoperability of STB.

Two CA specific profiling data proposed which are stored in SC by the operator and are used to configure the STB.

1. GN (Group Number) : For Filtering of EMMs.
2. Private data location: Filtering of private data from the specified location.

EMM message structure

TS Header	Zero byte	Table ID	Section syntax indicator + DVB/ISO reserved bits	Size (CA section length)	User group ID	CA data bytes	CRC
32 bits	8 bits	8 bits	4 bits	12 bits	16 bits	….	32 bits

Usage of group number (GN) for CAS

ECMs are per channel and EMMs are per subscriber containing encrypted SKs for all channels, the particular subscriber has subscribed for. In a conventional CAS, the EMM for a given subscriber is filtered and sent to SC. Here it is proposed to group a number of subscribers together (around 200-500 – operator specific) and send all EMMs corresponding to the subscribers having the same group number (GN) to the SCs. SC decodes only the EMMs meant for that subscriber. The GN and IK are kept totally uncorrelated. GN is also proposed to be kept independent of subscriber number.

The GN is sent from SC to STB after successful bi-directional authentication through safe channel. This marginally increase the BW requirement between STB and SC but enhances the security of the system as the potential attacker is never sure the EMM is for one or multiple subscriber and unauthorized decoding of EMM through any type of pattern matching becomes that much difficult.

Usage of private data for specific characterization of operator CAS

The operator (CAS supplier) may add some specific features and enhance the system security by using some private data (Fig 9). Although this is not a suggested mechanism, however a provision is kept, keeping in view that some CASs may be using this and providing an additional level of flexibility in the framework for the operator / CAS. This also ensures that CAS supplier has enough innovation space, maintains product characteristics & protects its differentiating property. The MPEG 2 TS specifications have provisions to add private data (other than ECM / EMM). After successful mutual authentication, Smart Card communicates to STB whether any private data exists or not; if exists the specific locations for the same. The STB 'CA-filter' accordingly configures itself to extract those private data from the received streams and send those to the Smart Card. The usage (what is done) with the private data in Smart card is known only to the operator Head–end and the valid smart card issued by the operator. Private data (if present) location is sent using user defined descriptors in tables of TS. The metadata transfer mechanism in TS is defined as part of interoperable specifications. This meta data used for decoding and filtering in STB and then sent to SC for further processing.

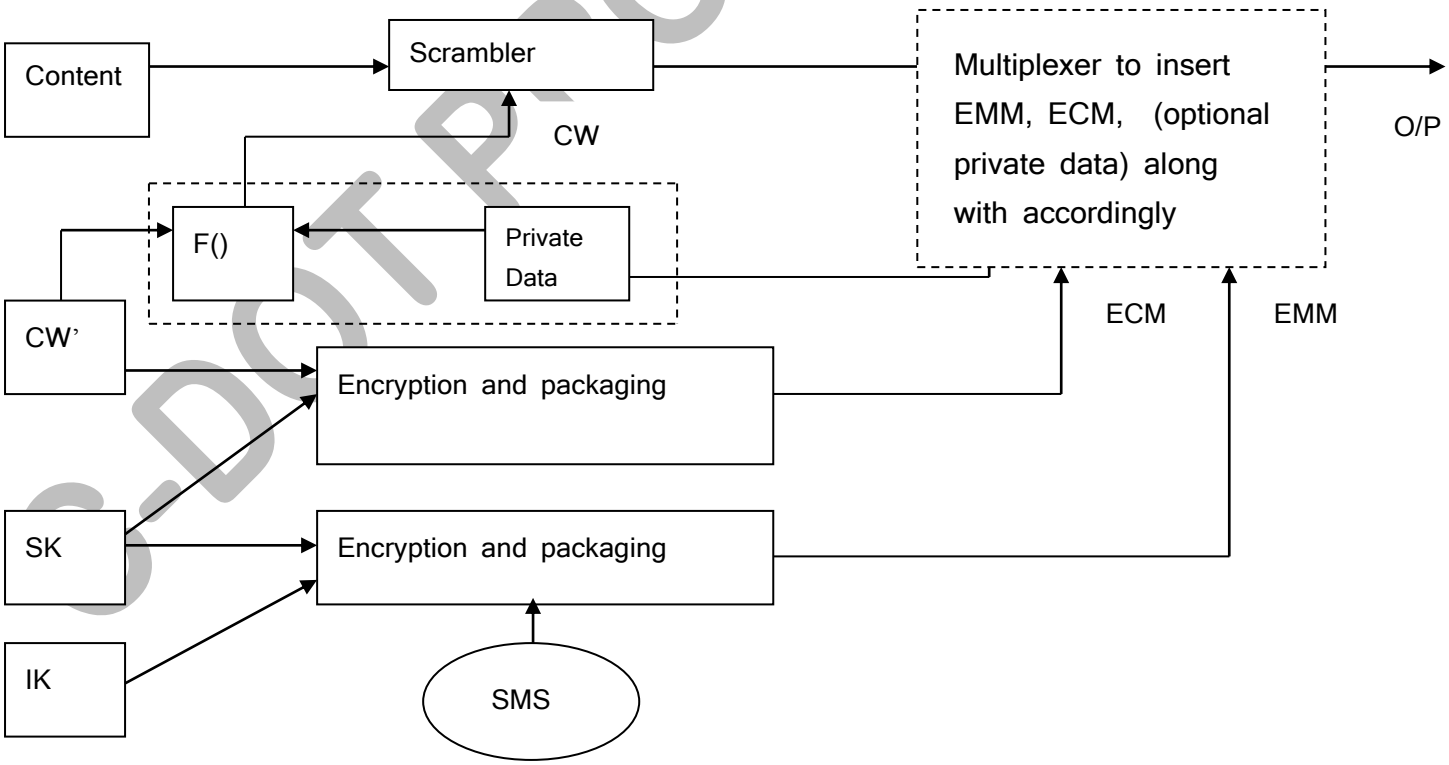


Fig 9: Possible usage of private data towards CAS

f. Configurable Universal CA (Conditional Access) filter:

Configurable universal CA filter is a part of Interoperable STB. In this scheme, the CA filter is specified in such a way that, it is capable of filtering the CA messages, which are relevant for the smart card presently put in the STB. That is, each time a different SC is put in the STB, the CA filter filters only the corresponding CA messages and sends those CA messages to SC for processing. The CA filter is thus made configurable.

The CA filter is made configurable w.r.t two parameters:

1. GN (Group Number): For Filtering of EMMs.
2. Private data location: Filtering of private data from the specified location.

When the CA-filter is configured by the data stored in the SC (and through OTA if needed), the CA filter filters the EMMs and 'private data' as required. The CA filter configurability is per operator as well as per subscriber basis. 'Private data location' is per operator basis and GN is per group of subscriber basis.

5.5 Approach With Respect to middleware and application interoperability issue:

- In this interoperable framework, middleware interoperability is achieved by following mechanisms:
  - The MPEG-2 TS should adhere to the rules defined in ISO 13818-1 and should contain the mandatory DVB-SI signaling as defined in EN 300 468. Also in order to move towards an interoperable regime, the broadcasters, network operators as well as STB manufacturers should follow the guidelines defined in ETSI TS 101 211 for SI implementation and shall also follow ETR-289.
  - Minimum additional recommendations taking into considerations the Indian Contexts.

- The implementation variations are programmatically read by STB as sent from the headend and partly also stored in the smart card.

All the tables shall follow the EN 300 468, TS101 211, ETR-289. The approach is that there will be a minimum set of compliance that needs to be adhered to by all the operators and STB manufacturers. Some of the specific aspects are additionally defined as part of interoperable framework (Refer section 6.c of this document). Apart from the minimum mandatory set, some of the implementation variations of the operators, can be programmatically read by the STB at the installation time to configure itself to the new operator's environments. This will ensure a smooth path towards STB interoperability; however in such a scheme, all the mandatory tables and the corresponding mandatory descriptors shall be adhered to by both operators as well as all STBs. This will ensure the STB middleware interoperability across multiple operators Headend. The minimum repetition periods as defined in TS 101 211 shall be adhered to by all operators and STB manufacturer. Wherever there are multiple options possible as per standards, the minimum set is defined taking into considerations, the interoperability requirements and Indian contexts. In-order to support co-existence of the legacy STB systems and the new interoperable STBs, the content of current TS implementation by the operators may continue to exist as it is and the additional common (i.e across the operators) TS encoding and decoding specifications required for the implementation of interoperable STB. After a defined cut off date, the control information related to legacy systems can be removed from the TS. After the defined cut off date, all the STBs in the network will be interoperable and the non-interoperable network elements will no longer be supported by any operator.

- Applications can be categorized into two broad types:
  - Electronic Program Guide (EPG)
  - Standalone GAMES those can be played on STB

Electronic Program Guide (EPG):

An electronic program guide (EPG) is an application used with digital set-top boxes to list current and scheduled programs that are or will be available on each channel and a short summary or commentary for each program. Primary functionality of EPG is to provide users with an easy to use, friendly interface in order to quickly access a program. The input to the application(EPG) comes by parsing the relevant PSI/SI tables those are part of the received stream from the headend. So, any EPG that runs on STB shall be able to provide basic information about program schedule etc. Basic minimum information can be defined as part of standard. It is envisaged that in the scenario of interoperable STB, there will be various types of STBs those will be available in the retail market. The range of STBs will be from a basic STB to a very high end STB. One fundamental requirement in such scenario is that all STBs (irrespective of basic or highend) shall be able to receive and decode signals and shall offer a basic user interface (EPG) to the end user for navigation of channels/programs. EPG in such situation is a feature of STB rather than that of a service provider. A sophisticated EPG in a high end STB shall be able to exploit all features that an operator may offer, however it is important to ensure that the basic EPG (in all STBs) shall be compatible and operational in all scenarios. However provision for down loading the operator specific EPG through OTA is also available in the framework. In such a case, different downloadable image is needed corresponding to each make of the STB for a given network. In such cases, the STB software is to be designed in such a way that the downloading and updating of EPG without replacing the middleware, is provisioned appropriately. For a java / MHP /HbbTV (etc.) enabled STB, there can be single downloadable image for a given feature set for a given operator.

Stand alone Games:

This can be provided as part of STBs, in that case it becomes a STB feature. If the operator wants to provide these “Gaming Applications”, there are two options:

a) It is required to adopt a standard platform by the STB manufacturers. Adaptation of an OS independent platform [similar to Java, MHP from ETSI, HbbTV is specifically designed for this purpose] to be used for application interoperability.
b) Each operator need to provide for downloading of machine readable gaming apps specifically implemented/designed for each type of STBs in the market.

5.6 Secure Boot & OTA

Secure Boot

In C-DOT defined framework, there is secure boot feature. But in this case, the secure boot mechanism is independent of any specific CAS. In this framework, there is security as per Manufacturer's signature. Any low level software (including boot code) to run, the code has to be signed by the manufacturer's key to ensure that no malicious boot code get's executed and only the boot code as authorized by the manufacturer gets executed. This scheme to be implemented by the STB manufacturers with the technical support from the SoC vendors and independent of operator or CAS.

OTA

In this framework, the OTA is primarily being used for downloading and updating of operator specific EPG and applications. ETSI TS 102 006, ISO/IEC 13818-6 are to be complied with for the purpose of OTA. Total middleware update is not allowed as part of OTA in interoperable framework. It is pertinent to mention here that, there will be a default EPG as part of the STB mandatory feature list. Some of the operator specific configurable data will be sent as part of normal TS (not part of normal OTA) in user defined descriptors standardised for this purpose, as part of the framework.

Secure OTA: For application level code to execute, the code is required to be signed by the manufacturer and operator for which the STB is presently installed / tuned to. This ensures that when the STB is installed for a given operator, the applications pertaining to only that operator (rectified by the corresponding STB manufacturer)

are executed. In the case of an evolved hardware architecture independent STB platform (like JAVA, HbbTV etc.), the applications can be independent of any specific STB manufacturer and those may be down loaded from authorized independent sources.

5.7 Approach With Respect to MPEG2/MPGE4 and DVB-S/DVB-S2 (in case of DTH):

The interoperable framework is agnostic to the media coding techniques and modulation schemes persay.

- MPEG2 and MPEG4 use the same transport mechanism [ISO 13818-1]; only the compression mechanisms are different. Hence incorporation of both the schemes are straight forward and very easily realizable in a ASIC / configurable silicon. Already such ICs are available off-the-shelf.
- DVB-S2 is an enhancement over DVB-S. This case is specific to DTH segment. It gives a Bandwidth saving of ~30%. DVB-S2 support backward compatibility with DVB-S. DVB-S2 is used as a zapper function on DVB-S. Silicon /ASICs available supporting both.
- With most of the existing SoCs, these can very easily be handled in a seamless way.

6. Feature Requirements for the Ecosystem Entities towards Implementation of STB Interoperability

In order to achieve STB interoperability and to implement the above mentioned framework, each of the entities in the total ecosystem needs to satisfy some of the requirements. These are needed in order to meet all the functional requirements and also to maintain high level of content security.

6.a) Requirements to be met by STB SoC

Cryptographic requirements for STB SoC are detailed here. The functional modules as required towards implementation of STB interoperability and to maintain content security are listed below. These functional modules to be implemented in secure hardware (preferably) or through a secure processor (many of these features are available in most of the existing commercial STB SoCs).

Modules required in SOC:

- OTP ROM (size= 5 kB) (secure storage of data: unmodifyable& secure read)
- RSA hardware (encryption/decryption/verification)
- AES hardware (encryption/decryption)

Data routings required (Fig 10)

- OTP ROM to RSA key input (direct path in SOC)
- RAM to RSA key input
- RAM to RSA data input
- RSA (sk) decryption output to AES key input (direct path in SOC)
- RSA (pk/sk) decryption output to AES data input (direct path in SOC)
- RSA (sk) encryption output to RAM
- RSA (pk) verification output(0/1) to RAM
- RAM to AES data input
- AES output to RAM

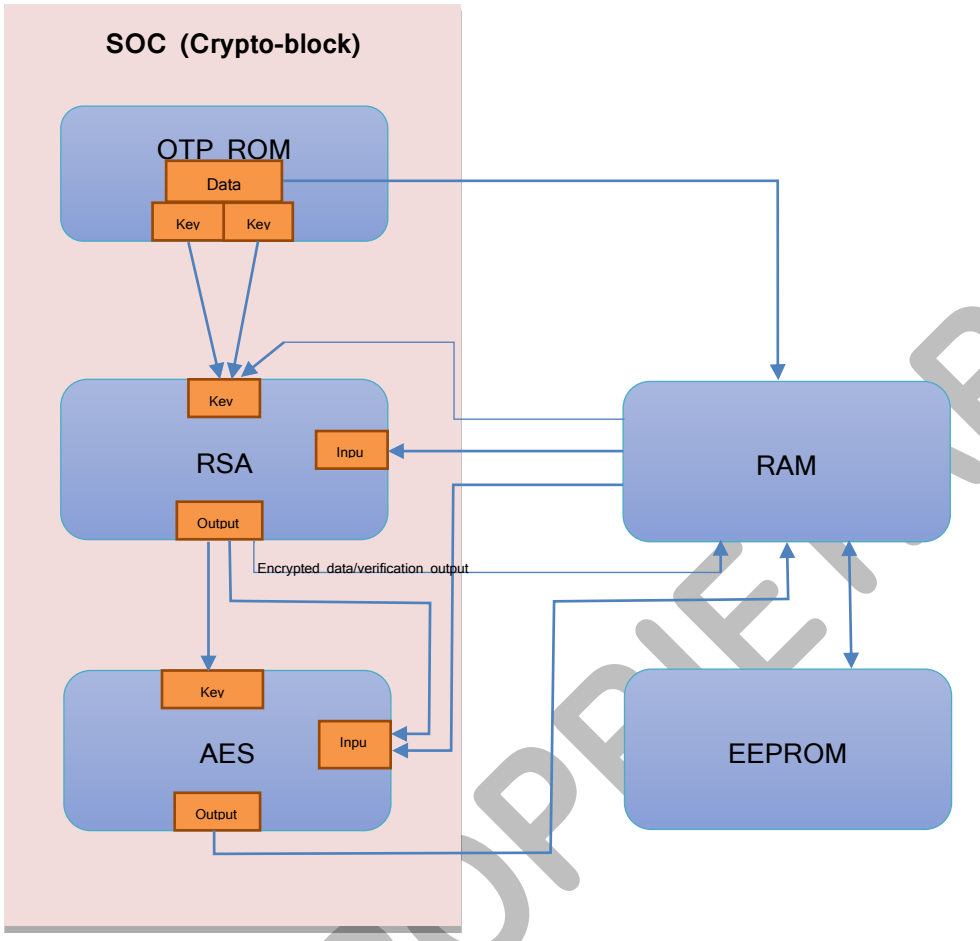


Figure 10: Cryptographic requirements for STB SOC

Note:

1. * Only encrypted data or verification output should be routed from RSA hardware to RAM. Decrypted data should be given to only AES HW.
2. Exact implementations may vary satisfying the security requirements of key storage / exchange / processing.

6.b) Requirements to be met by CAS

I. Requirements Towards Bidirectional Authentication:

1) Operator (CAS vendor for a given operator) should obtain the valid certificate and a RSA [2048-bit] keypair from Trusted Authority.
2) The operator should be able to generate new and unique RSA [2048-bit] keypair for each smartcard it provides to the customer.
3) The operator should also generate the certificate corresponding to each keypair. These certificates will contain operator's signature signed using operator's private key.
4) The operator must fuse the private key and certificate of each smartcard along with its own certificate in the OTP ROM located inside smartcard chip. The private key should not be accessible to any software module. Only RSA hardware should have access to it.
5) After sharing session key with STB securely, it must be configured as input key to AES hardware for future use (and erase it from RAM after that).

Software requirements:

Headend: RSA keypair generator,
RSA certificate generator
Smartcard: Smartcard side version of Bidirectional authentication protocol

Hardware requirements:

Headend: Random number generator (for RSA key generation)
Smartcard: OTP ROM (size = 3229 Bytes*):
Operator and SC certificates: 523x2 = 1046 Bytes
SC Private Key: 1732 Bytes
TA Public Key: 451 Bytes
RSA (Encryption/Decryption/Verification) hardware,
AES (encryption/decryption) hardware

Note: * Size of Operator and SC certificates can change depending on the certificate structure used and fields added to it. Hence the final size of 3229 Bytes for ROM is minimum memory required for bidirectional authentication to work.

II. Requirements towards OTP based security enhancement scheme

1) Operator has to maintain following information about each of its registered user:

- Basic customer information (Name, Address, email-id, etc.)
- Registered mobile number
- Smartcard information (smartcard number, smartcard version, etc.)
- STB information acquired during registration process (STB-ID, STB Public key, etc.)
- Remaining OTP validity
- Number of OTP requests by the user for a particular duration

2) Operator has to finalize a value for OTP validity for its subscribers.

3) Operator has to generate N-digit random number and 16 Byte random periodic key for each OTP request it receives from every subscriber.

4) Operator should have access rights for all STB manufacturers' portal for getting STB certificates.

Software requirements:

Headend: Subscriber database,
Operator side version of OTP based STB-Smartcard-operator binding protocol

Smartcard: Smartcard side version of OTP based STB-Smartcard-operator binding protocol

Hardware requirements:

Headend: Random number generator (for OTP and periodic key generation)
RSA (encryption/verification) hardware

Smartcard: AES (decryption/encryption) hardware,
OTP ROM (size = 16 Bytes): User key (16 Bytes)

III. Requirements towards Interoperability scheme

1) The periodic key sent to the subscriber during OTP based binding process should be used for encrypting individual subscriber-specific entitlement messages.
2) The entitlement message structure should be in accordance with the guidelines provided for the same.
3) For maximum security, all the processing of entitlement messages should be carried out inside the smartcard and descrambling keys (Control words) should be sent to the STB in encrypted form using the session key shared during bidirectional authentication process.
4) Messages are filtered in the STB based on the user-group id it is pre-configured to. This user-group id can be a static or dynamic based on the CAS vendor's addressing mechanism. The configuration of user-group id can take place during the OTP based binding process with the use of trigger EMM. CAS vendor may use its proprietary logic for this configuration provided that final entitlement messages follow the packet structure guidelines.

EMM Packet structure:

Field	TS Header	Zero byte	Table ID	Section syntax indicator + DVB/ISO reserved bits	Size (CA section length)	User group ID	…	CRC
Size	32 bits	8 bits	8 bits	4 bits	12 bits	16 bits	…	32 bits

As seen above, 16 bit User Group ID is additionally introduced as per the requirement of interoperable framework to process/filter the EMMs based on operator specific grouping of subscriber in a given network.

6.c) Middleware interoperability

The MPEG-2 TS should adhere to the rules defined in ISO 13818-1 and should contain the mandatory DVB-SI signaling as defined in EN 300 468.

Also in order to move towards an interoperable regime, the broadcasters, network operators as well as STB manufacturers should follow the guidelines defined in ETSI TS 101 211 for SI implementation. In this section, the requirements specifically for achieving middleware interoperability are detailed. Due to implementation variations and the prevailing flexibilities in the specifications, achieving interoperability of STB from middleware point of view still requires some adaptation. In C-DOT approach to interoperability, it is mandatory to adhere to ETSI TS 101 211, ETR -289, set of recommendations as defined in this section and the few implementation variations are proposed to be sent by the operators over the TS (in specified tables) in a specified way. When an interoperable STB gets connected to a new network (different operator), the STB programmatically reads the operator specific variations from the air/cable TS (can be partly in Smart Card as well) and configures itself according to the variations in the operator specific middleware. There are user defined descriptors available as per the prevailing mentioned standards, and some of these descriptors used in specific tables can be standardized to carry the Meta data related to operator specific middleware variations.

The following are these recommended rules specified and shall be met by both the operators and STBs towards achieving interoperability. However this is not an exhaustive list.

1. Every PSI/SI table inserted into the TS (i.e in the form of sections) shall not be scrambled and should strictly follow the recommendations defined in EN 300 468 and TS 101 211, including the table repetition rates.

2. In addition, the broadcasters, network operators as well as STB manufacturers should follow the additional recommendations specified in Table 1 for STB interoperability requirement.

Table 1: TS Tables encoding/decoding specifications for interoperability

S.No	Feature	Mandatory Compliance	Specific Recommendation	Remarks/Restrictions
1	Service Multiplexing & De-multiplexing	Receive and process SI (Service Information) as laid down in EN 300 468 & TS 101 211		PAT, PMT, CAT, NIT, SDT, EIT and TOT are mandatory whereas BAT, TDT and other tables are optional.
2	Conditional Access	Descramble services scrambled in accordance with ETR 289 (DVB-CSA) and other recommendations of ETR -289 for CA data.	16 bit Group ID is added in the EMM structure.	At present, DVB-CSA v2 is recommended.
3	Service list & description	1. Service description shall be identified	Service list shall be derived from the loop of service_id and	service_list_descriptor (tag= 0x41) defined in NIT/BAT is not to be used for obtaining the

		using the service_descriptor (tag=0x48) as defined in SDT (PID=17).	service_descriptor in SDT.	service list.
4	Service Categorization	Services shall be classified using the content_descriptor (tag= 0x54) as defined in EN 300 468 for usage in EIT (PID=18)..	For details on Categorization, Refer section 6.c.i below	content_descriptor or an user_defined_descriptor defined in the SDT (PID=17) shall not be used by the receiver for classifying services. Also the bouquets in BAT (PID=17) shall not be used for classification.
5	Electronic Program Guide (EPG)	EPG data shall be derived using the EIT schedule table on PID=18.		EPG service signaling either in NIT or BAT first loop using linkage_descriptor (tag=0x4A, linkage_type=0x02) and defined as a service in PMT shall not be used for deriving EPG information.
6	Logical Channel		Channel	user_defined_descripto

	Numbers (LCNs)		numbering shall be allocated using logical_channel_descriptor (tag=0x83) defined in the second loop of NIT (PID=16) or BAT (PID=17). See below LCN section for more details. The LCN descriptor is additionally used here and is not part of EN 300 468. However it is defined in AS 4599 for DVBT. Refer Section 6.c.ii below.	r defined in NIT/SDT/BAT or any other proprietary mechanisms shall not be used for LCN.
7	Data services	Receive & process Data streams compliant to EN 301 192 &TR 101 202		
8	Subtitles	EN 300 743 – Subtitling systems		
9	System Software Update (SSU)	TS 102 006 using DSM-CC (ISO/IEC 13818-		Only applications such as EPG is allowed to be downloaded /

		6)		updated through OTA.
10	Private Data	Meta Data related to Private data location in TS is through user defined descriptors.	Descriptor Tag range : 0X80 – 0XFE	The usage of Private data is operator specific and to be consumed in the Smart Card.

6.c.i Categorization of the Services:

The services defined within the network can be classified using the EIT present/following table. For categorizing services, the receiver should process and decode the content_descriptor in the EIT p/f table.

The content_descriptor as defined in EN 300 468 for usage in EIT, shall be used for defining the categorization details of each service. All the values for the fields content_nibble_level_1 and content_nibble_level_2 in the content_descriptor shall be used and decoded as it defined in EN 300 468, except for the user defined mechanism (i.e content_nibble_level_1=0xf and content_nibble_level_2=0x0 to 0xf), which shall not be used by the receiver for identifying any service classification information.

In addition, the 8-bit field user_byte in the content_descriptor shall be used for defining the classification based on regional languages. The allocations of the codes for the user_byte field need to be defined for the Indian regional languages with inputs from broadcasters and operators as the same field is currently used by them in a different way for categorization.

Any bouquets defined in the BAT Table shall not be used by the receiver for classification because of the unique bouquet_ids being used by the broadcasters and N/W operators.

6.c.ii Logical Channel Numbering (LCN):

LCN allows the broadcasters in ordering their services/channels. Each service/channel by the broadcaster may be allocated a unique default channel

number within the same network_id (except when its value is zero). The allocation of these LCNs shall be defined in the logical_channel_descriptor (tag=0x83) and the descriptor shall be inserted in the 2nd descriptor loop of either the NIT table or BAT table. The receiver shall use the logical channel descriptor defined in NIT table at higher priority to process and decode the logical channel numbers, followed by the BAT table.

The syntax and semantics of the logical_channel_descriptor is indicated in Table 2, as follows;

Table 2: Logical channel descriptor Syntax

Syntax	No. of bits	Identifier
logical_channel_descriptor() {	8	uimsbf
descriptor_tag	8	uimsbf
descriptor_length		
for (i=0; i<N;i++) {	16	uimsbf
service_id	1	bslbf
visible_service_flag	5	bslbf
reserved	10	uimsbf
logical_channel_number		
}		
}		

descriptor_tag: This shall be assigned to be 0x83.

service_id: This is a 16-bit field which serves as a label to identify this service from any other service within the Transport Stream. The service_id is the same as the program_number in the corresponding PMT. Services shall be included irrespective of their running status.

visible_service_flag: This 1-bit field when set to '1' indicates that the service is normally visible and selectable via the service list. By setting this field to "0", the service and the associated LCN, should not be visible or accessible to the viewer in the normal Service Lists and EPG. While all the services in the multiplex are allocated with LCNs by the broadcasters, not all the services may be intended to be seen or selected by the viewer. Certain services like multimedia streams, data streams, SSU, games etc may need to be concealed from the service list and made invisible to the viewer.

reserved: All the "reserved" 5 bits shall be set to "1".

logical_channel_number: It is a 10-bit field which provides the channel number for the service_id, to indicate the broadcaster preference ordering services.

Operator specific data in STB:

a. Frequency, Modulation, Symbol rate and bandwidth
    - Can be configured through the installation setup.
b. User's Group ID and the Table_IDs to use in EMM filtering
    - Table_IDs as defined in the standard can be used, whereas User's group ID defined in the EMM message is operator choice and shall be configurable to use with EMM filter using either from TS or OTP binding or any other operator specific addressing mechanisms in place.
    - CAS vendor may use its proprietary logic for this user group ID configuration provided that final entitlement messages follow the EMM packet structure guidelines as defined.

6.d) Requirements to be met by STB manufacturer/STB OEMs

1. STB manufacturers shall get manufacturer id along with private and public key pair from TA.
2. STB manufacturer will be getting the infrastructure details needed towards the generation of Private/Public Key pair for each of the STBs it manufactures from TA. STB manufacturer will be working as secondary Trusted Authority.
3. STB manufacturer will be given the tool chain by the SoC vendor / OEMs on how to embed the private keys/data in the secure memory of each of the STBs it produces.
4. The interoperable logic (software code) is developed by the STB OEMs as per the defined open standard (to be defined as per interoperable framework).
5. OEMs will be developing the middleware / applications as per the middleware recommendations as given in section 6.c above. Middleware can also be developed by any third party following the open recommendation and that can be integrated by OEMs.
6. The STB manufacturer will maintain a portal and will provide the public key of the STBs it manufactured against the STB id printed on STB. This is needed for mobile OTP based security enhancements. This information will be provided by the operators through the proper credential verifications.

6.e) Requirements to be met by TA (Trusted Authority)

1. TA shall be a National entity and is the root of trust for all the keys generated either by the operators or by the manufacturers.
2. TA will generate Private/Public Key pair and Ids for Operators and Manufacturers
3. TA will provide all the infrastructural details needed by STB manufacturer and Operators towards key pair generations.

Only the functional requirements w.r.t. interoperable framework is mentioned above. The generic operational/security requirements are to be met by TA / Secondary TAs.

Conclusions:

In order to achieve technical interoperability of STB, it is required that every entity in the total signal/content chain satisfy the recommendations towards interoperability. After detailed analysis, it has been concluded that, to attain STB interoperability, it is very much necessary that a total interoperable framework is developed and mandated. In this interoperable framework, the major focus has been on achieving interoperability for basic STBs. In this scheme, it is also taken care that smooth migration towards an interoperable regime is possible, so far as field proliferation is concerned. In order to implement this framework by the relevant stake holders and to achieve STB interoperability, it is necessary that corresponding total specifications detailing the messages and frame structures are formulated and adhered to by all the stakeholders.

References:

1. TRAI Pre-Consultation Paper On Set Top Box Interoperability dated 04/04/2016.
2. ETSI TS 101 211
3. ETSI TS 103 162 V1.1.1 (2010-10)
4. IS 16128 : 2013: Indian Standard, STB FOR MPEG4 DIGITAL CABLE TV SERVICES.
5. ETSI EN 300 429: Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for cable systems
6. EN 300468: Digital video broadcasting (DVB); Specification for service information (SI) in DVB systems
7. C-DOT Patent : US8978057B2
8. EN 300421 Digital video broadcasting (DVB); Framing structure. channel coding and modulation for 11/12 GHz satellite services
9. ETSI EN 302 307: Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)
10. ISO/IEC 13818-1: Information technology - Generic coding of moving pictures and associated audio information: Systems.
11. EN 301192 Digital video broadcasting (DVB); Specification for data broadcasting
12. ETR 289 Digital video broadcasting (DVB); Support for use of scrambling and conditional access (CA) within digital broadcasting systems
13. IS 15377:2003 : Digital Set Top Box for Direct-to-Home (DTH) Services - Specification