



**Telecom Regulatory Authority of India**



**Consultation Paper**  
**On**  
**Framework for Technical Compliance of Conditional**  
**Access System (CAS) and Subscriber Management**  
**Systems (SMS) for Broadcasting & Cable Services**

**22nd April 2020**

Mahanagar Doorsanchar Bhawan

Jawahar Lal Nehru Marg

New Delhi-110002

Website: [www.trai.gov.in](http://www.trai.gov.in)

**Written comments on the Consultation Paper are invited from the stakeholders by 20<sup>th</sup> May, 2020 and counter comments, if any, may be submitted by 3<sup>rd</sup> June 2020. Comments and counter comments will be posted on TRAI's website [www.traigov.in](http://www.traigov.in) . The comments and counter comments may be sent, preferably in electronic form to Shri Anil Kumar Bhardwaj, Advisor (B&CS), Telecom Regulatory Authority of India, on the e-mail:- [advbcs-2@traigov.in](mailto:advbcs-2@traigov.in) or [jadvisor-bcs@traigov.in](mailto:jadvisor-bcs@traigov.in) .**

**For any clarification/ information, please contact Shri Anil Kumar Bhardwaj, Advisor (B&CS) at Tel. No.: +91-11-23237922, Fax: +91-11-23220442.**

## Contents

<b>Chapter</b>	<b>Topic</b>	<b>Page No.</b>
Chapter 1	Introduction	04
Chapter 2	Functions of CAS/SMS and Extant Regulatory Provisions	12
Chapter 3	Issues Related to Sub-Standard CAS & SMS	25
Chapter 4	Testing, Certification and Accreditation Agencies	35
Chapter 5	Issues for Consultation	45
	List of Abbreviations	48
Annexure I	Schedule III, Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017	51
Annexure II	Comparison of Standard and Sub-standard CAS	55
Annexure III	International Experience with Standards-Making Process	59

## **CHAPTER 1 INTRODUCTION**

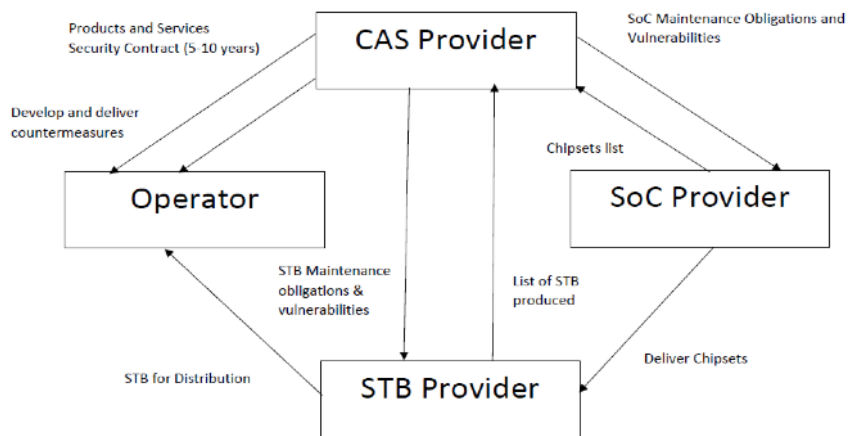
- 1.1** Television has been one of the most popular medium of mass communication and entertainment. India is no exception to this global trend. The Indian TV industry has, over the years, developed into world's second largest television viewing universe globally with 836 million TV viewers<sup>1</sup>. As per the industry estimates, at the end of year 2018 there were 298 million households in India, out of which 197 million<sup>2</sup> households had television sets.
- 1.2** Since 2004, regulatory framework for broadcasting and cable services has evolved over time through various timely interventions by Telecom Regulatory Authority of India (TRAI) for orderly growth of the sector by way of new regulations and making amendments to the existing ones. The first major structural and technology reform in cable TV industry was the introduction of Digital Addressable System in 2011-12.
- 1.3** Pursuant to TRAI recommendations dated 5<sup>th</sup> August 2010 on Digital Addressable Systems (DAS), the Government amended the Cable TV Regulation Act, 1995. The Government issued notification dated 11<sup>th</sup> November 2011, which laid down the roadmap for implementation of digitalization in the Cable Television sector in four phases starting from June 2012. Digitalization in the cable sector was implemented in four phases and it has been completed all over the country by 31<sup>st</sup> March 2017. Other distribution platforms like Direct To Home (DTH), Internet Protocol Television (IPTV) and Headend In The Sky (HITS) already use digital addressable systems.
- 1.4** Digital Addressable Systems (DAS) provide subscribers with a degree of choice that they did not have so far. DAS has multiple advantages over the analogue system. It enables expanded capacity in terms of number of

---

<sup>1</sup> BARC Report, Broadcast India 2018 Survey, July 2018.

<sup>2</sup> FICCI-EY Report, 2019

television channels providing more choices to consumers and better viewing quality etc. DAS also brings in transparency among the service providers and meets the ultimate objective of allowing a consumer specific choice of television channels. DAS environment consists of the Conditional Access System (CAS), which is the cornerstone of transmission system as it is responsible for the encryption of content. CAS enables secure delivery of the television channels to only the authorized subscribers. Another key component of the DAS ecosystem is the Subscriber Management System (SMS), which acts as the management module. The SMS is responsible for activation/deactivation of STBs, managing subscriber information, channel information, billing and other such activities. Working together, CAS and SMS systems play a pivotal role in the service delivery value chain. A Distribution Platform Owner depends on the CAS and SMS providers to introduce new features and fight piracy. The relationship and interdependencies of key players is illustrated in Figure 1<sup>3</sup>. More details of the DAS ecosystem are provided in next chapter.



**Figure 1 Relationship of Key Players in a Pay TV Ecosystem**

**1.5** India, being a large market, has seen almost all global players in CAS/SMS eco-system operating in the country. There are more than fifteen CAS

<sup>3</sup> Image courtesy: M/s Nagravision, Kudelski group.

systems deployed by the Distribution Platform Owners (Direct to Home Players and Multi-Systems Operators). A list of currently deployed CAS in India, as per industry information, is provided in Table1.

<b>Sl. No.</b>	<b>CAS Platform</b>	<b>Country of Origin</b>	<b>Type</b>	<b>Secure IP Core/ RoT</b>
1	NDS-Cisco	Israel/US	Advanced Embedded	Yes
2	Nagra-Kudelski	Switzerland	Advanced Embedded	Yes
3	Irdeto	Netherland	Advanced Embedded	Yes
4	Conax-Kudelski	Norway	Advanced Embedded	Yes
5	Verimatrix	US	Advanced Embedded	No
6	iCAS-Bydesign	India	Advanced Embedded	No
7	Crytogaurd	Sweden	Advanced Embedded	No
8	Arris-Latens	US	Advanced Embedded	Yes
9	Safeview	Spain/India	Non Advanced	No
10	ABV	China	Non Advanced	No
11	NSTV	China	Non Advanced	No
12	GosCAS	China	Non Advanced	No
13	Sumavision	China	Non Advanced	No
14	LRIPL-Only1	India	Non Advanced	No
15	Logic Eastern-OneCAS	India	Non Advanced	No
16	Others	Mixed	Non Advanced	No

*Table1: Conditional Access Systems operational in India*

**1.6** Further, DPOs have deployed different types of Subscriber Management System (SMS) as depicted in Table 2. Such SMS have varying capabilities without any direct linkage to the CASs deployed.

<b>S.No.</b>	<b>Company/ Product Name</b>	<b>Country of Origin</b>
1.	Aplomb	India
2.	Ask	India
3.	BITS	India
4.	Cryptoguard	Sweden
5.	Drops	India
6.	Efficiense Gospel	China
7.	e-Life	India
8.	Ensurity Dexin	China
9.	iCAS	India
10.	ICORE	India
11.	Impact	India
12.	ITP	India
13.	Jacon	Czech Republic
14.	Kingwon	China
15.	Lightware Digital	India
16.	Logic Eastern	India
17.	Magnaquest	India
18.	Media Nucleus	India
19.	Neeladri Software	India
20.	Paycable	India
21.	Payconnect	India
22.	Preciso	India
23.	Reliable Soft	India
24.	Ridsys	India
25.	SecureTV	China
26.	SkyLink	India
27.	Sprintsoft	India
28.	Synergy	India
29.	WI Digital	India
30.	Sumavision	China

*Table 2: Subscriber Management Systems operational in India*

- 1.7** Introduction of Digital Addressable System (DAS) has enabled addressability, transparency, high channel carrying capacity and provided technical feasibility to offer choice to the consumers. As the technology helps in extending television signals over long distances, large multi-city, multi-state Multi-Systems Operators (MSOs) have emerged. To extend the full benefits of digitalization to the consumers and also to address various issues of the sector, TRAI notified a comprehensive regulatory framework comprising of the Interconnection Regulations<sup>4</sup>, the Quality of Service Regulations<sup>5</sup> and the Tariff Order<sup>6</sup> in March 2017.
- 1.8** The new framework engenders the “must provide” and “must carry” principles in the broadcasting sector ensuring non-discrimination among service providers. The framework provides for enabling mechanism to introduce transparency in the sector. Further, the accounting, billing and payment of revenue among stakeholders is now primarily based on actual number of subscribers. There are enabling provisions for mandatory audit of the DPO systems to provide requisite assurance to broadcasters. Schedule III (**Annexure I**) of the Interconnection Regulation specifies the benchmark features/ technical criteria that the systems are required to comply with. In addition, there are provisions in Schedule III that entail CAS and SMS systems to conform to certain technical features to check the piracy. The regulatory framework establishes a trust based transparent regime.
- 1.9** As mentioned earlier, CAS and SMS are pivotal for the Digital Addressable Broadcast eco-system. These are responsible for delivery of the content in a secure & encrypted manner only to authorized subscribers. CAS and SMS also help a DPO to take-out various reports as regards the subscriber

---

<sup>4</sup> The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017

[https://main.traigov.in/sites/default/files/Interconnection\\_Regulation\\_03\\_mar\\_2917.pdf](https://main.traigov.in/sites/default/files/Interconnection_Regulation_03_mar_2917.pdf) ;

<sup>5</sup> The Telecommunication (Broadcasting and cable) Services Standards of Quality of Service and Consumer Protection (Addressable Systems) Regulations, 2017

[https://main.traigov.in/sites/default/files/QOS\\_Regulation\\_03\\_03\\_2017.pdf](https://main.traigov.in/sites/default/files/QOS_Regulation_03_03_2017.pdf)

<sup>6</sup> Telecommunication (Broadcasting and Cable) Services (Eighth) (Addressable Systems) Tariff Order, 2017 (1 of 2017) [https://main.traigov.in/sites/default/files/Tariff\\_Order\\_English\\_3%20March\\_2017.pdf](https://main.traigov.in/sites/default/files/Tariff_Order_English_3%20March_2017.pdf)



management and authorisation, including the broadcaster's (Television Channel wise) subscription report. The requirements to be complied by the DAS including those of CAS and SMS are specified in Schedule III of the Interconnection Regulation, 2017. However, the schedule III requirements are quite generic in nature, thereby allowing all type of CAS and SMS systems to exist in the eco-system. Some CASs are using advanced embedded security while others are based on non-standard security solutions as can be seen from Table 1. Any systems that deploy sub-standard solutions can be vulnerable to hacking, thereby putting content security at risk. Moreover, majority of the CAS companies do not have their own SMS, Middleware (MW) and User Interface (UI). This increases the dependencies of the MSOs on the Third party (TP) software solutions. As majority of the MSOs lack in-house technical expertise, they face many problems due to sub-standard solutions. Service and support related issues from such third party vendors cause poor outcomes for the consumers.

**1.10** The Authority receives hundreds of complaints every year from various broadcasters as regards the piracy and distribution of pirated signals. In general, such cases are examined by the concerned Authorized Officers as per Cable Television Networks (Regulation) Act, 1995. However, as per analysis much of such piracy occurs due to deployment of CAS that do not fully comply with security protocols as per extant standards and regulatory provisions. Even though Cable Television Networks Rules, 1994 clearly stipulate for transmission of content in encrypted manner, broadcasters and DPOs have also been raising complaints regarding transmission of pirated content in various regions. issue was raised by stakeholders as one of the major concerns during the annual Chief Executive Officers' interaction with the Authority held on January 14, 2020. Pursuant to a detailed deliberation, all present agreed that establishing a framework to ensure compliance with minimum technical

specifications in accordance with regulatory framework is necessary for CAS, SMS and DRM.

**1.11** Therefore, the Authority has examined the issues arising out of deployment of various CAS and SMS across the country. Based on preliminary analysis following issues emerge:

- Some DPOs could not implement various parameters prescribed in QoS regulations. The CAS/ SMS did not support the prescribed features in some cases. In other cases, though the CAS/ SMS could support the feature, implementation required manual configuration by the supplier /vendor. Such vendors sought very high charges to make such configurable changes.
- Due to the limitations of SMS, a few DPOs could not provide required choice to the customers.
- Few of the DPOs could not implement a standard SMS based activation/deactivation of channels due to absence of such feature in the SMS or non-support of such commands by the CAS system.
- Many small distributors could not standardise the code for addition/ removal of Television channels.
- The extant framework mandates provision of channel 999 as Consumer Information Channel. Few DPOs couldn't provide sufficient feature-based information on channel no. 999 due to limitations of their systems. Therefore, some distributors cannot abide by the regulatory provisions due to limitations of their CAS/ SMS systems.
- There are operation related issues like non-availability of billing features in the software systems.
- Very long turn-around time by CAS / SMS systems' suppliers causing delayed implementation of extant regulations.

- 1.12** All these concerns reflect a need for compliance with minimum technical specifications before a CAS/SMS is installed in Cable TV network.
- 1.13** With this background, TRAI has initiated this consultation on *suo-motu* basis to deliberate upon the issues related to CAS and SMS systems, their underlying factors and possible remedial measures. Ensuing chapters deal with functioning of important constituents of Digital Addressable Systems and challenges posed by non-standard systems in the network. Chapter 2 deals with use of CAS & SMS and regulatory provisions. Chapter 3 discusses the issues related to sub-standard CAS and SMS. Chapter 4 provides a brief account of testing, certification and accreditation agencies across globe and in India. Chapter 5 presents the summary of issues for consultation.

## **CHAPTER 2**

### **FUNCTIONS OF CAS/SMS AND EXTANT REGULATORY PROVISIONS**

- 2.1** In a Digital Addressable System (DAS) based environment, CAS and SMS are an integral part and the quality of service is dependent on the CAS and SMS systems being deployed by the DPO. Therefore, in order to ensure seamless transmission of signals of television channel from broadcaster to consumer, maintaining the addressability and preventing piracy, it is necessary that certain benchmark for the CAS and SMS systems are put into place. The extant regulatory framework vide Schedule III (**Annexure I**) provides for a macro level parameters/ features that the DPOs must comply with.
- 2.2** The regulations provide for certain checks under the provisions of audit of the DPO systems that entail testing of the relevant features as prescribed under the schedule III. This chapter describes the CAS and SMS systems in detail. In addition, all other peripheral sub-systems of an addressable system are also described herein for a general overview. Thereafter the extant provisions and features of Audit are presented to comprehend the existing checks/ tests.
- 2.3** Addressability is the ability of a digital device to individually respond to a message sent to many similar devices. In the pay television distribution framework (DTH or Cable or through IPTV etc.) an addressable system enables and controls the distribution of television channels, by encrypting the signal and ensuring only authorized users can receive channels using a set-top-box (STB) and TV set.
- 2.4** The Interconnection Regulation, 2017 defines addressable system as:

*“addressable system” means an electronic device (which includes hardware and its associated software) or more than one electronic device put in an integrated system through which transmission of programmes including re-transmission of signals of television channels can be done in encrypted form, which can be decoded by the device or devices at the premises of the*

*subscriber within the limits of the authorization made, on the choice and request of such subscriber, by the distributor of television channels;*

**2.5** The Cable Television Networks (Regulation) Amendment Act, 2011 defines addressable system as:

*“an electronic device (which includes hardware and its associated software) or more than one electronic device put in an integrated system through which signals of cable television network can be sent in encrypted form, which can be decoded by the device or devices, having an activated Conditional Access System at the premises of the subscriber within the limits of authorization made, through the Conditional Access System and the subscriber management system, on the explicit choice and request of such subscriber, by the cable operator to the subscriber”.*

## **2.6 Conditional Access System (CAS):**

By definition a Conditional Access means, “the access is based upon certain condition”. Under a Conditional Access System only an authorized receiver/STB can decrypt the broadcast content. Essentially, CAS ensures that content delivery pipe from the operator to the STB is secure and provides a mechanism of addressing each STB uniquely. CAS comprises a combination of scrambling and encryption to prevent unauthorized reception. Scrambling renders the sound, pictures and data unintelligible while protection of the secret keys during transmission is achieved through encryption.

### 2.6.1 Scrambling and Encryption:

Making the TV signal un-viewable selectively, is achieved by a combination of scrambling and encryption. The Conditional Access System works by using a set of secret keys for scrambling or encryption. These keys are protected and hidden by various methods and are securely carried from the headend to the Set Top Box (STB)/subscriber. The keys are used to scramble the signal, making it accessible only to authorized STBs.

(i) Scrambling:

Scrambling is a process of protecting some or all components of a service to cope with unauthorized access by using cipher encoding under the control of the CAS at the sending end. The Common Scrambling Algorithm (CSA) is the algorithm used in the DVB digital television broadcasting for encryption. CSA was specified by European Telecommunications Standards Institute (ETSI) and adopted by the DVB consortium in May 1994. At present there are three types of CSA: CSA1, CSA2 and CSA3. The CSA operates on the payload of a Transport Stream (TS) packet in the case of TS level scrambling. CSA1 used 48 bit key, CSA2 used 64 bit key and CSA3 uses a 128-bit key (Control Word) to encrypt and decrypt data blocks. The Control Word (CW) is generated automatically in such a way that successive values are not predictable. In order for the receiver to unscramble the data stream, it must have information about the current value of the control word.

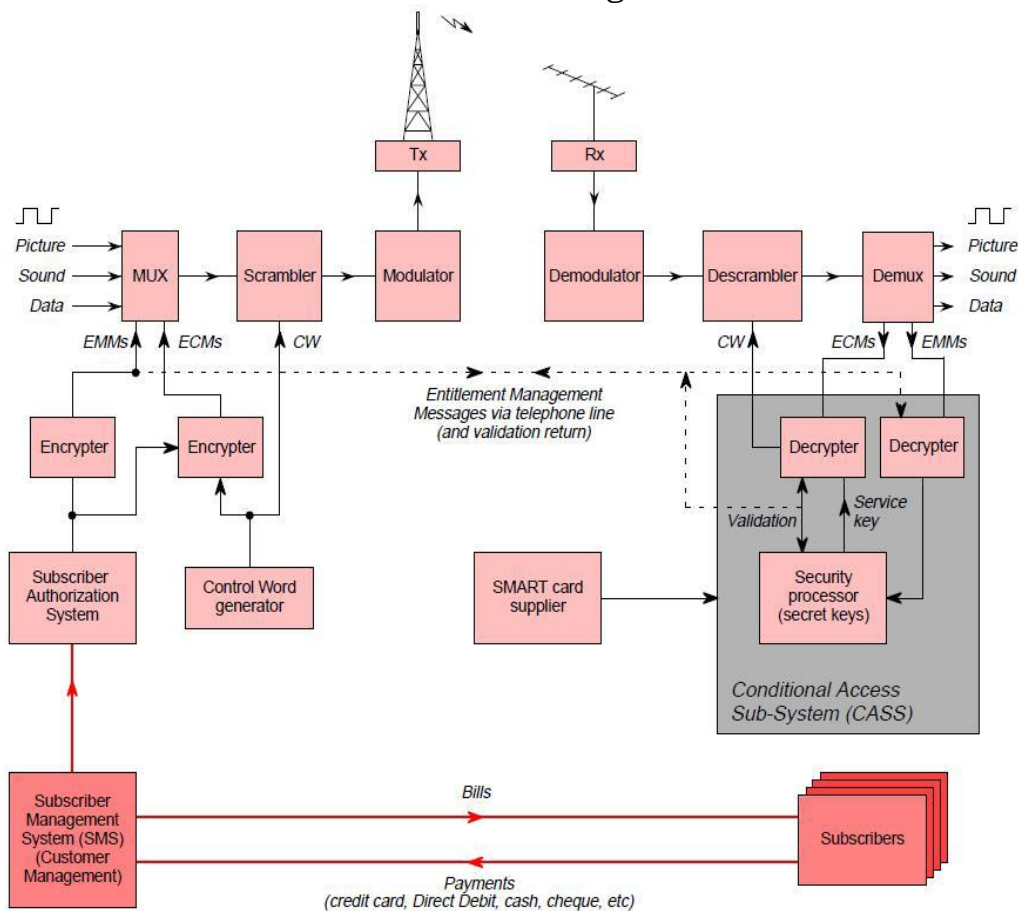
(ii) Encryption:

Encryption is used to protect the control word during transmission to the receiver. Encrypted information (the control word) is sent out using two separate methods.

- **Entitlement Control Message:** The control word is encrypted as an Entitlement Control Message (ECM). The Conditional Access (CA) subsystem in the receiver will decrypt the control word only when it is authorized to do so.
- **Entitlement Management Message:** The authorization to decrypt is sent to the receiver in the form of an Entitlement Management Message (EMM). The EMMs are specific to each subscriber, as identified by the smart card in his receiver. New EMMs are issued much less frequently than ECMs; typically, at intervals ranging from about every 10 minutes to up to once every 6 weeks.

The Security of a CA System depends on the Algorithm used for ECM, EMM Encryption. The contents of ECMs and EMMs are not standardized and each Conditional Access System uses different ECMs and EMMs. In fact, the security of a given CA system depends primarily on the efficiency of the algorithm used for ECM, EMM encryption. Such algorithms are closely guarded secrets of the company. The CA module in the STB carries relevant ECM, EMM decryption algorithms.

Majority of the CAS deployed in India work either on CSA1 or CSA2. CSA3, though the advanced algorithm, may not be supported by and most of the scramblers, STBs and other legacy hardware currently deployed in India. Moreover, adopting CSA3 also has significant financial implications as it would require replacement of deployed scramblers, STBs and other hardware. The basic structure of CAS is shown in Figure 27:



<sup>7</sup> Image courtesy: Bureau of Indian Standards (BIS)

*Figure 2: CAS schematic diagram*

### 2.6.2 Subscriber Authorization System (SAS):

The SAS is a subsystem of the CA system that translates the information about the subscriber into an EMM, when the Subscriber Management System requests for it. The SAS also ensures that the subscriber's security module receives the authorization needed to view the programs. Further, the SAS acts as a backup system in case of failure.

### 2.6.3 Security Module:

There are basically three types of CAS implementations deployed in Indian market. First one is carded CAS where a viewing card or smartcard is required to decrypt the encrypted signals. Owing to security concerns regarding exposure of secure keys during transmission between the card and the STB processor, preference of the industry shifted to the second type of CAS, viz. chip based, cardless CAS. Cardless CAS has two variants. One in which the decryption algorithm is stored on the common RAM of the STB in the form of software. Such CASs are regarded as non-advanced type being more vulnerable to hacking. In the third type of CAS, the secured security module is integrated within the SoC the STB for decrypting the content. These “advanced embedded” CASs are regarded as the most robust from content security point of view.

## **2.7 Subscriber Management System (SMS):**

The SMS is essentially the management center of the CAS. It is combination of hardware and software integrated with CAS server. SMS stores and manages details of each subscriber, and the TV channels that are subscribed to by the subscriber. Based on the channels that the subscriber has paid for, the SMS asks for Entitlement Management Messages (EMM) from the Subscriber Authorization System (SAS). It also generates the bill for LCOs as well as Subscriber enabling MSO to charge them accordingly.

### **Functions of SMS**

As front end to the operator's equipment, SMS performs practically all



operational functions required for managing day-to-day operation of the business. Important functions carried out by the SMS are described below.

#### 2.7.1 Subscriber related

SMS deals with subscriber (STB) activation/deactivation, bulk subscriber suspend/resume, blacklisting STBs, etc. It also stores and manages subscriber data such as subscriber name, subscriber Mobile Number, subscriber address etc. These entries can be updated whenever changes take place. SMS server generates unique customer ID for each subscriber and carries out STB pairing function wherein customer id is paired with the STB number and the Smartcard number (for card-based STB) or Chip id number. This is an important functionality related to activation/deactivation or blacklisting of STB.

#### 2.7.2 Local Cable Operators (LCO) related

SMS contains data of the Operators like Operator Code, Operator Name, Operator Address etc. SMS contains Admin ID for MSO and MSO can generate LCO IDs for his linked operators, thus enabling them with activation/deactivation etc. of their STBs. LCO can also download all his STBs details with subscriber name and address.

#### 2.7.3 Billing System

SMS provides a host of billing functions such as itemized billing, bill scheduling, supporting multiple tax systems etc.

#### 2.7.4 Stock Management

By using SMS, the MSO can manage his stock for the STBs. SMS can individually show the entries of Activated STBs, Deactivated STBs, Faulty STBs and Blacklisted STBs.

#### 2.7.5 Channel Information

SMS stores and manages all the information about channels available on

the MSO platform, package, bouquet or scheme creation etc. It enables management of channels and program bouquets subscribed by individual subscribers.

Since SMS is not a standardized product, different versions deployed by operators can provide various other functions and features such as subscriber alerts, LCO applications etc. SMS is also responsible for enabling and managing the important functions of fingerprinting and OSDs (On Screen Display) etc.

## **2.8 Other Components in Television Distribution Network:**

In addition to the CAS and SMS, there are various other components comprising the television broadcast network, which are briefly touched upon below. The consultation paper on 'Interoperability of Set-Top-Box' describes these components in greater details. The same can be accessed at [https://main.trai.gov.in/sites/default/files/CP\\_STB\\_Interoperable\\_11112019.pdf](https://main.trai.gov.in/sites/default/files/CP_STB_Interoperable_11112019.pdf).

### **2.8.1 Set Top Box (STB)**

A Set-top box is a device that receives digital signal, decodes and displays it on television. Based on the transmission type, i.e. cable, satellite or terrestrial, the STBs are based on corresponding DVB standards, i.e. DVB-C, DVB-S or DVB-T. Their hardware configuration generally remains same except for tuner and demodulator, as it depends on the transmission scheme. The STB retrieves the TV channels and other services from this signal through demodulation, descrambling and decompression.

### **2.8.2 Middleware**

Middleware is the software that sits on top of the operating system (OS) in an STB. It allows a content developer to work without having to consider the low-level issues for an STB. It runs between OS/device drivers and the

application. Middleware makes it easier to write complex applications and it allows portability across hardware and operating systems.

### 2.8.3 System on Chip (SoC)

System on Chip (SoC) is one of the most critical components of the broadcast service delivery chain. SoC is designed according to the selected CAS and plays crucial part in establishing the robustness of the system for content security. Thus, the Advanced embedded type CAS would require the CAS specific secret keys to be fused in the SoC making it secure against hacking.

## **2.9 Regulatory Framework Prescribed by TRAI**

2.9.1 It is evident from the description of the key components in the preceding sections that the CAS and the SMS are central to the Pay TV networks. They are the key elements governing content security and proper accounting of subscription and revenue. Accordingly, the regulatory framework notified by TRAI incorporates provisions regarding the minimum requirements to be complied by the CAS and SMS deployed by the DPOs.

2.9.2 The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 dated 3<sup>rd</sup> March 2017 (herein after the Interconnection Regulations 2017) notified by TRAI cover technical and commercial arrangements between the Broadcaster & the Distributor for providing television services to the consumers. Subsequently, TRAI also issued Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations, 2019 (7 of 2019) on 30<sup>th</sup> October 2019 (herein after called Amendment Regulations).

2.9.3 As per the Regulations, the digital addressable systems deployed by the DPOs for distribution of television channels through cable & satellite are required to meet the minimum criteria as stated in the Schedule III of the Regulations. The addressable system requirement as provided for in Schedule III to be complied by Distributor of television channels is attached as **Annexure I**.

2.9.4 In order to ensure compliance with these minimum criteria, the authority notified The Telecommunication (Broadcasting and Cable) Services Audit Manual<sup>8</sup> dated 8th November 2019 which provides formalities to be followed for the Audit initiated by the Distribution Platform Operator (DPO) vide sub-Regulation (1) of Regulation 15 or by the Broadcaster vide sub-Regulation (7) of Regulation 10 and sub- Regulation (2) of Regulation 15.

**Pre-Signal Audit:**

2.9.5 A pre-signal audit is carried out before the content acquisition by the Distribution Platform Operator (DPO) from respective broadcaster, otherwise is called as compliance audit. Pre-signal/compliance audit may be carried out as per Schedule III mentioned in the Interconnection Regulations 2017.

2.9.6 In accordance to the sub-regulation (6) of regulation 10 of the Interconnection Regulation 2017, every distributor of television channels before requesting signals of television channels from a broadcaster shall ensure that the addressable systems to be used for distribution of television channels meet the requirements as specified in the Schedule III of the Interconnection Regulations 2017. For ensuring the same, DPO can get the pre-signal Audit conducted either by BECIL or any other agency empaneled by TRAI. The DPO has to provide its declaration in writing to

---

<sup>8</sup> The Audit Manual is only a guidance document for stakeholders and auditors. The manual does not supersede any provision(s) of the extant regulations.

broadcaster regarding Schedule III compliance along with below mentioned documents for requesting signals along with other requisite documents:

- CAS certificate provided by vendor.
- SMS certificate provided by vendor.
- STB certificate provided by vendor.
- BIS compliance certificate.

2.9.7 Regulation 10(7) of the Interconnection Regulations 2017 inter-alia provides if a broadcaster, without prejudice to the time limit specified in Sub-Regulation (2) of Regulation 10, is of the opinion that the addressable system, being used by the distributor for distribution of television channels, does not meet the requirements specified in the Schedule III of the Interconnection Regulations 2017, it may cause audit of the addressable system and provide a copy of the report prepared by the auditor to the distributor. However, it is important to note the proviso to the sub-regulation (7)<sup>9</sup> of Regulation 10, before instituting such audit by the broadcaster.

### **Subscription Audit**

2.9.8 Regulation 15 of the Interconnection Regulations 2017 provides for subscription audit, after provisioning of signals by the broadcaster, by every distributor of television channels, for audit of its subscriber management system, conditional access system and other related systems by an auditor, once in a calendar year, to verify that the monthly subscription reports made available by the distributor to the broadcasters are complete, true and correct, and issue an audit report to this effect to

---

<sup>9</sup> Proviso to Sub Reg (7) of Regulation 10 "Provided that unless the configuration or the version of the addressable system of the distributor has been changed after issuance of the report by the auditor, the broadcaster, before providing signals of television channel shall not cause audit of the addressable system of the distributor if the addressable system of such distributor has been audited during the last one year by M/s. Broadcast Engineering Consultants India Limited, or any other auditor empaneled by the Authority and the distributor produces a copy of such report as a proof of conformance to the requirements specified in the Schedule III.

each broadcaster with whom it has entered into an interconnection agreement.

**2.9.9** In case the broadcaster is not satisfied with the audit report received under Regulation 15 (1) or, if in the opinion of a broadcaster the addressable system being used by the distributor does not meet the specified requirements, it shall be permissible to the broadcaster, as per sub-Regulation (2) of Regulation 15, after communicating the reasons in writing to the distributor, to audit the subscriber management system, conditional access system and other related systems of the DPO, not more than once in a calendar year. The regulation also permits the broadcaster under proviso as per Sub-Regulation (2) of Regulation 15 to disconnect signals of television channels, after giving written notice of three weeks to the distributor, if such audit reveals that the addressable system being used by the distributor does not meet the requirements specified in the Schedule III.

**2.10** Hence, Schedule III of Interconnection Regulation, 2017 provides the minimum criteria to be met by the digital addressable systems deployed by the DPOs for distribution of television channels through cable & satellite and sets into place a statutory framework that ensures that any changes, modification and alterations made to the configuration or version of the addressable system (CAS, SMS and other related systems<sup>10</sup>) of the DPO and/or distribution network of DPOs do not in any way compromise the system and all the equipment including software meets the statutory compliance requirements.

**2.11** Further, effective compliance of statutory provisions is ensured through the comprehensive Audit Manual<sup>11</sup> published by the Authority. It creates a common framework and uniformity in the technical and subscription audit

---

<sup>10</sup> 'Other related system' means any related component which has commercial implication or affects technical compliance of the DAS system.

<sup>11</sup> The Audit Manual is a guidance document for stakeholders. This manual does not supersede any provision(s) of the extant regulations.

process for all digital addressable systems used in the broadcasting sector. It provides a well-defined audit procedure and a check list of all the equipment/software/accessories, etc. used in digital addressable system. The audit manual builds the trust and confidence among all stakeholders in broadcasting sector, which in turn, results in reducing disputes among the stakeholders arising during provisioning of TV channel or at the time of renewal of Interconnection agreements, etc.

- 2.12** With the extant policy and regulatory framework in place and supported by technology, distribution of television services should ideally be a smooth and problem free operation. The underlying technologies have undergone much advancement over the years to enable secure transmission of content with adequate protection to the authorized subscriber. However, despite being crucial in provisioning quality services to end-consumers, there are hardly any prescribed benchmarks for digital addressable systems.

Though Schedule III of the Interconnection Regulations 2017 sets out the minimum requirements to be met by digital addressable systems, there are several issues that arise due of deployment of non-tested and non-certified CAS and SMS. Since, Schedule III requirements are generic in nature, it allows all type of CAS and SMS systems to exist in the eco-system. Most of the major vendors undertake elaborate measures and use advanced embedded security to ensure adequate mechanism towards content security. However, quite-a-few vendors do not take such measures and deploy systems based on non-standard security solutions, vulnerable to hacking. Such systems put the content security at risk, thereby distorting the markets. It is important to note that market functions as a whole and any such distortion leads to market failures.

- 2.13** The regulatory framework released by TRAI establishes a trust based transparent regime and provides opportunities to aspiring entrepreneurs to enter into television distribution business. Such new entrants may lack

technical expertise and experience. Such players are likely to be beguiled by cheaper products, therefore exposing their networks to piracy and other contraventions. Many a time DPOs choose some CAS and SMS systems not fully aware about the technical complexities. However, subsequently they suffer when either broadcasters deny them the feed of TV signals in pretext that they do not meet mandatory technical requirements or OEMs of such CAS and SMS vendors ask more money to provide required upgrade to fulfill technical requirements. Protection of such MSOs is also important so that all CAS/ SMS system operational in cable TV network adhere to minimum technical requirements.

**2.14** There are instances, where unscrupulous operators take advantage of the gaps in the operational and oversight mechanisms and playing around the system. The following chapter deals with instances of issues raised by various stakeholders in this regard and discusses related issues.

**2.15** Apropos discussions in the above sections, the issues for consultation are:

**Q1. List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?**

**Q2. As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?**



## **CHAPTER 3**

### **ISSUES RELATED TO SUB-STANDARD CAS & SMS**

The Cable Television Networks (Regulation) Act, 1995, the permission/ license to DPOs and the extant regulatory framework lay down requirements to be met by the Addressable Systems. However, broadcasters and distributors regularly raise issues arising out of deployment of sub-standard systems. The issues reported are described herein under three broad heads viz. Security related issues, Operational issues and Support related issues.

#### **3.1 Security-related issues:**

##### **3.1.1 Transmission of unencrypted signals, unauthorized transmission of signals**

This is by far the most recurring issue reported by various broadcasters from various territories. It is also probably the most critical issue as it amounts to theft of content and thereby results in direct loss of revenue to the concerned broadcaster and also to the government. The transmission of unencrypted signals is a clear violation of section 4A of the Cable Television Networks (Regulation) Act, 1995. It enables unauthorized reception of the content and thereby amounts to infringement of provisions of the Indian Copyrights Act, 1957 and constitutes a criminal offence resulting in unlawful gain to the offender and loss to the affected stakeholders.

##### **3.1.2 Finger printing/watermarking not supported by the system**

Schedule III of the Interconnection Regulation (**Annexure I**) has specific provisions for fingerprinting (both visible and covert) and watermarking to be complied by the distribution equipment. This is a critical tool to identify the source of a breach of security if it happens and thereby taking corrective measures such as barring content access by the compromised STBs and blacklisting them, apart from other actions. A timely action is

important in minimizing the extent of loss due to piracy, especially in case of time-critical content, such as sports events. Non-compliance of fingerprinting/ watermarking deprives the affected parties of this damage control mechanism.

### 3.1.3 Cloning of STB:

Even though Schedule III categorically mandates that each STB should be individually addressable, there are reported cases of cloning of STBs, wherein by hacking of secure key of a STB, it was cloned into several STBs while only the hacked STB was reflected in the system. This is another instance of piracy resulting in leakage of revenue.

## **3.2 Operational issues:**

### 3.2.1 Integration issues between CAS and SMS

Interconnection Regulations mandate that activation and deactivation of STBs should be done with commands of the SMS and that CAS should not have the facility to activate/deactivate STBs. As such, the SMS and CAS should be in absolute synchronization at all times. However, issues are raised from time to time from field in this regard. It is alleged that in few cases, there may be mirror SMS which, while able to configure subscribers, does not reflect subscribers' information in main subscriber database. This issue has multiple implications. Firstly, it results in improper reporting of subscription figures. As revenue sharing under the regulatory framework is subscription based, this has serious implications. On the other hand, synchronization issue also has implications on service provisioning to consumer. For example, this may result in a situation where a program has been subscribed to a particular customer/STB but due to integration problem it may not reflect in CAS and the consumer may remain deprived of the service. The converse is also possible wherein a customer may be availing subscription to certain program(s) while the

same are not reflected in SMS. This issue can lead to serious discrepancies during bulk activation/deactivation.

### 3.2.2 Absence of creation/modification logs in the system

Absence of proper, tamper-proof log in the CAS/SMS has serious consequences. The presence of temper proof logs gives the confidence to technical audit team that nothing is being hidden and helps in complete investigations. Absence of temper proof logs raises suspicion of wrongdoing. It provides opportunity to an unscrupulous operator to manipulate subscription data and thereby distort the revenue reports. Another way in which it provides a window for manipulation is through the Access Criteria defined in the CAS. Access criteria controls all the service ids of the channels and decides whether an STB will have access to certain channels or not based upon its entitlement. If the access criteria is disabled then the STB will have complete access to all the channels and this will not reflect in the CAS and SMS reports. In the absence of proper log, there would be no mechanism to check whether the access criteria is manipulated anytime to under report the active subscriber count.

### 3.2.3 Absence of blacklisting feature in SMS

As described earlier, fingerprinting and watermarking are important tools in identifying the source of piracy and the compromised STBs and taking corrective action by restricting access and blacklisting them. However, there are instances where the SMS does not have the facility to blacklist such compromised STBs, thereby causing irreparable harm.

## **3.3 Support related issues:**

In addition to the security related and operational threats as summarized above, there are instances of complaints raised by MSOs regarding support-related issues from CAS/SMS vendors. Specifically, such complaints either pertain to delay or lack of support in relation to needed

software modification in the system in compliance to a license or regulatory requirement. Pursuant to coming into effect of the new regulatory framework, there have been cases, where a DPO could not implement the new billing regime timely. Not only the DPO faced regulatory actions, it also incurred losses in terms of higher pay-out to broadcasters as well-as the consumers, as it failed to activate channels as per consumer choice(s). There have been reports where the vendor sought exorbitant charges for a modification or an upgrade as the DPO became a captive customer.

### **3.4 Challenges associated with sub-standard systems:**

Analysis of the reported issues as summarized above reveals there are primarily two ways in which these issues can be manifested. One is due to deployment of sub-standard systems (CAS/SMS) in the field and the other is due to fraudulent operation of the systems. As far as fraudulent operation of the systems with a malicious intent is concerned, inspections and operational oversight mechanism can probably be the only effective way to curb the menace with relevant technical support and audit trail. However, creating a framework that prevents deployment of sub-standard systems in the network can be expected to bring a preventive control as far as potential threats arising due to vulnerability of such systems to hacking is concerned. Further, it may also be argued that support related issues can perhaps be addressed more effectively through suitable policy framework. Few of the ways in which sub-standard systems put the ecosystem to risk are described below:

#### **3.4.1 No protection against Control Word (CW) Sharing**

CW is not sent in an encrypted format in the Entitlement Control Message (ECM) in substandard CASs. It is possible to get the CW by snooping methods. If CW is not protected, then it would allow the Local

Cable Operator (LCO)/ Hacker/to redistribute the signals without the knowledge of the Operator/Broadcaster and get profited from it.

#### 3.4.2 Weak encryption of Entitlement Control Message (ECM) and Entitlement Management Message (EMM)

ECM and EMM are not encrypted in sub-standard CAS. It does not have mechanism for Custom EMM generation and handling. If ECM/EMM are not protected, then it would allow the hackers to redistribute the signals unlawfully.

#### 3.4.3 Unsecure Boot Loader

Sub-standard CAS does not have secure boot loader and hence it allows non-authenticated software to boot up the STB. Further it allows malicious software to be downloaded in an STB. Non-Secure Boot Loader can put investment of the operator on the STB at risk because if a malicious software is running on the STB it can make the boxes to behave abnormally and can even make STBs in operation to stop working completely, making the operator to re-invest in buying all the boxes once again. Several complaints have been received from operators alleging malpractices by such substandard CASs, owing to which support issues are faced by the concerned MSOs.

Non-secure Boot Loader can also result in releasing the control word which would allow the end user to redistribute the signals without the knowledge of the Operator/Broadcaster.

#### 3.4.4 Poor Support for Detection of Security Breach

It has been mentioned in Chapter 1 that CASs deployed have varying level of security robustness against piracy, varying from Advanced embedded type to non-advanced. CASs with non-advanced security are obviously more vulnerable to piracy. Fingerprinting/watermarking mechanisms do provide a mechanism to block access of content to

compromised devices/ network in case of a security breach. However, sub-standard CASs may not even have fingerprinting mechanisms. Owing to these factors content can be pirated and redistributed on various online as well as offline modes mechanisms without the knowledge of the operator or the broadcaster.

#### 3.4.5 Blacklisting of STBs

Sub-standard CASs allow compromised STBs to continue to run in the network, as they do not have a provision for blacklisting of smart cards or ID's of the STBs, thereby allowing content piracy to continue without the knowledge of the operator or the broadcaster.

#### 3.4.6 Issues with CAS Server Hardware

Sub-standard CAS are not deployed on head-end server hardware specifically supplied by CAS provider and it is possible to deploy sub-standard CAS in just any commercially available generic servers thereby removing any extra layer of data/cyber security and increasing the probability of any backdoors and malicious software deployments.

#### 3.4.7 Integration Issues with the SMS

Sub-standard CAS normally has integration issues with the SMS. Such CAS does not have consistency in term of integration and is not able to accept/recognize commands from SMS on regular basis or during bulk activation/deactivation. Any activation/deactivation command or any other command sent from SMS can be rejected or not accepted by CAS. This will result into reconciliation issues between CAS and SMS because the same STB can be found in active state in CAS whereas in SMS it will be showing inactive or vice versa.

#### 3.4.8 Auto Expiry and Disentitlement of Services

In sub-standard CAS the Set Top Box (STB) does not get disentitled to the services automatically on the expiry date set at the beginning of the subscription period and needs a command from the Subscriber Management System (SMS) to get disentitled. Therefore, substandard CASs increases the traffic of the SMS commands to send entitlement and de-entitlement commands every month for every customer. It results in significant bandwidth consumption if the network has few thousand customers and few hundred services and packages to subscribe.

#### 3.4.9 Issues with Addressability

In sub-standard CAS the EMM addressability in individuals/groups/region/global/LCO is not achievable. The definition of the groups may not be based on rules definitions such as geographic locations based on pin code, city, etc. Consequently, the operator and broadcaster lose the control on the field network and its STBs.

#### 3.4.10 Generation of CAS Reports & data bases in editable formats

Sub-standard CAS/SMS deployment results into increasing the probability of misreporting the usage and subscription numbers, as it also generates CAS reports in editable Formats such as csv, excel. It generates logs which are accessible by any user or operator for manipulation and/or modification. This may result into revenue loss to the operator, broadcaster as well as to the government in form of taxes. Further, the Sub-standard CASs do not have an option to back up all the critical data as per the configuration.

#### 3.4.11 B Mails/Alerts

Sub-standard CAS makes it difficult to send message to end user which may be critical to continue the service or inform the end user of some life-threatening disaster/calamity etc.

A comparison of the standard and sub-standard CASs on the lines of major areas of concern is provided at **Annexure II**, indicating associated risk factors and their threat level.<sup>12</sup>

### **3.5 Implications and possible threats from deployment of sub-standard CAS/ SMS**

The issues reported from time to time indicate that a lot of proprietary solutions have made way into the Indian market offering cheap security. Because of this, different stakeholders in the ecosystem suffer, not just the end consumer, but also the service providers and the Government.

#### **3.5.1 Impact on the Consumer**

Sub-standard CAS increases the workload of the operator and creates a confusion among the end consumers who may get non-uniform services from the same operator. It may result in frequent disruptions and hence poor Quality of Service (QoS) for the end consumer.

The consumers get locked in with STBs with limited functionality because of sub-standard proprietary software, which in turn results into the wastage of money for the end consumer as they may have to replace the STB many times during the subscription period.

#### **3.5.2 Impact on the Broadcaster**

Broadcasters and content developers are impacted directly by deployment of sub-standard CAS/SMS, as security of their content is compromised. It leads to content piracy and redistribution without the knowledge and permission of the broadcaster and the operator.

---

<sup>12</sup> Source: Broadcast Engineering Consultants India Limited (BECIL)



Further, certain features such as LCN etc. can't be implemented seamlessly across all STBs in a network owing to sub-standard proprietary software.

Sub-Standard CAS/SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the broadcaster and disputes with the operators in cases of under/excess billing.

Frequent disruption of services results into creating a lot of issues on the ground as the revenue collection is disrupted. It may attract lawsuits against the operators which may have the potential to disrupt their entire business operations

### 3.5.3 Impact on MSO/DPO/Pay TV Distributor

Since majority of the CAS companies do not have their own SMS, Middleware (MW) and User Interface (UI), it increases the dependency of the MSOs on several Third party (TP) software solution providers. Since most of the MSOs lack in technical expertise as they have migrated from Analog Cable TV regime, they fall prey to sub-standard solutions and face support issues subsequently.

MSOs get locked down to only one kind of boxes/STB original equipment manufacturer (OEM) with non-standard implementation of middleware features and incur high maintenance overhead to maintain and execute such proprietary software. It increases their operational cost as technical issues arise. Their flexibility to extend features is reduced.

Additionally, it creates tension with broadcasters, as there is a potential to manipulate the readings and log numbers which may result into misrepresentation of the data and may affect the revenue for all parties concerned due to excess/under billing.

Since deployment of a substandard proprietary software can result into content leakage and piracy, it may lead to various legal and commercial

actions by the content owner and hence disrupt the complete operations of the MSOs.

Further, in absence of Hardware Specifications and Performance Parameter standards, MSO may keep on investing into poor/cheap quality hardware which results into wastage of time, the generation of a lot of e-waste, resource wastages in terms of financial resources, human resources as well as management resources.

#### 3.5.4 Impact on the Government

Sub-standard CASs defeat the very purpose of the Government of India's DAS (Digital Addressable System) initiative. Sub-standard CAS/SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the operator, broadcaster as well as to the government in form of taxes.

Further, CASs which follow accepted global standards can be useful when changes from middleware perspective, such as STB Interoperability are implemented by the government.

#### 3.6 Apropos discussions in the above sections, the issues for consultation are:

**Q3. Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?**

**Q4. What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?**

## CHAPTER 4

### TESTING, CERTIFICATION & ACCREDITATION AGENCIES

- 4.1** In view of the discussions in the preceding chapter, there may be a need to consider developing an overarching framework for standardization, certification and testing of various components of addressable systems i.e. CAS and SMS. Further, effective compliance of statutory framework is essential to build the trust and confidence among all stakeholders.
- 4.2** In India, the technical benchmarks and standards for security testing of digital addressable systems are not in place at present. Therefore, it would be appropriate to study the process of development of a technical framework, its adoption and implementation consisting of testing methodology, certification and accreditation.
- 4.3** A general process of establishing a testing framework follows different modes, including the following, amongst others:
- a. Emergence as de facto framework/ standard: tradition, market domination etc.
  - b. Developed by a common industry body:
    - in a closed consensus process: Restricted membership and often having formal procedures for due process among voting members.
    - in a full consensus process: Open to all interested and qualified parties and with formal procedures for due-process considerations.
  - c. Written by a government or regulatory body.
  - d. Written by a corporation, union, trade association etc.
- 4.4** Once the framework/ test document is ready and notified, a formal **certification** adds credibility to the process. It is the provision whereby an independent body gives a written assurance i.e. a certificate that the product, service or system in question meets specific requirements. **Accreditation** is the formal recognition by an independent body, generally

known as an accreditation body that a certification body operates according to international standards.

## **4.5 Standardization, Certification and Accreditation Process in India**

### **4.5.1 Bureau of Indian Standards (BIS)**

The standards process in India is largely government led by Bureau of Indian Standards publishing majority of products and services related Standards. The Bureau of Indian Standards (BIS) is the National Standards Body of India established under an Act of Parliament (The Bureau of Indian Standards Act, 1986, revised as The Bureau of Indian Standards Act, 2016) and represented as the India member on ISO. Only standards published by BIS have the status of Indian Standards. BIS is involved in various activities like standards formulation, certification of products, hallmarking, testing and calibration scheme and more. More details on the structure and functioning of BIS can be accessed at <https://bis.gov.in>.

- **Product Certification by BIS**

Product Certification by BIS has been put into place since July 2013 and is intended to guarantee quality, safety and reliability. BIS Certification is provided in India under different types of schemes as follows:

- a. Product Certification
- b. Systems Certification
- c. Foreign Manufacturers Certification Scheme (FMCS)

BIS certification is normally voluntary in nature. However, BIS requires compulsory certification and registration for products which impact the health and safety of consumers. BIS Act, 2016 empowers Central Government to notify compulsory BIS Certification or Registration of a product. Penal provisions for better and effective compliance and to enable

compounding of offences for violations have also been made stringent under BIS Act, 2016. Compulsory Registration Scheme (CRS) has been adopted by ministries such as Ministry of Electronics & Information Technology (MeitY) and Ministry of New and Renewable Energy (MNRE) for mandating product conformance to Indian Standards. The grant of licence and its operation under Compulsory Registration Scheme are carried out as per the conformity assessment scheme under Scheme - II of Schedule - II of BIS (Conformity Assessment) Regulations, 2018.<sup>13</sup>

Further, government agencies may make it compulsory for foreign manufacturers to obtain a BIS product certification license for the products they intend to export to India under the Foreign Manufacturers Certification Scheme (FMCS). Under the provisions of this scheme, license is granted to a Foreign Manufacturer for use of Standard Mark on a product that conforms to an Indian Standard.

#### 4.5.2 Quality Council of India (QCI)

QCI is an apex body responsible for establishing a transparent and credible accreditation system. QCI is governed by a Council comprising of 38 members and has an equal representation of Government, Industry and other Stakeholders. QCI has four Accreditation Boards involved in accreditation programmes. Each board is functionally independent and works within their core area of expertise.

- a. National Accreditation Board for Certification Bodies (NABCB)
- b. National Accreditation Board for testing & calibration Laboratories (NABL)
- c. National Accreditation Board for Hospitals and healthcare providers (NABH)
- d. National Accreditation Board for Education & Training (NABET)

---

<sup>13</sup>[https://www.crsbis.in/BIS/app\\_srv/tdc/gl/docs/BIS\\_Conformity\\_Assessment\\_Regulation\\_2018\\_Gazette\\_Notification.pdf#page=221](https://www.crsbis.in/BIS/app_srv/tdc/gl/docs/BIS_Conformity_Assessment_Regulation_2018_Gazette_Notification.pdf#page=221)

Further, QCI develops accreditation standards to support accreditation programs where such standards are not available at the national/international level.

Apart from BIS, there are other sector specific SDOs (Standard Development Organisations) which are involved in the process of developing or formulation of standards, testing and certification.

#### 4.5.3 Telecommunication Engineering Centre (TEC)

Telecommunication Engineering Centre (TEC) is a technical body representing the interest of Department of Telecom (DoT), Ministry of Communications, Government of India. The main services of TEC include:

- Standardisation

Prepare specification of common standards about Telecom network equipment, services and interoperability. Published specifications of TEC are of three types namely Generic Requirements (GRs), Interface Requirements (IRs) and Service Requirements (SR). The List of Technical specifications including Standards published by TEC can be accessed at <http://www.tec.gov.in/complete-list/>.

- Testing and Certification

The Indian Telegraph (Amendment) Rules, 2017<sup>14</sup> provide that every telecom equipment must undergo prior mandatory testing and certification. TEC has been designated as the Telegraph Authority for the purpose of administration of Mandatory Testing and Certification of Telecom Equipment (MTCTE) procedure and Surveillance Procedure, and for formulation of Essential Requirements. More details on the working of TEC can be accessed at <http://www.tec.gov.in/certification-approval-procedure/>.

---

<sup>14</sup> Indian Telegraph (Amendment) Rules, 2017<sup>14</sup>, ART XI, Testing & Certification of Telegraph, (Rule 528 to 537)

#### 4.5.4 Standardization Testing and Quality Certification (STQC) Directorate

Standardization Testing and Quality Certification (STQC) Directorate is an attached office of the Ministry of Electronics and Information Technology, Government of India, which provides quality assurance and conformity assessment services in the area of Electronics and Information Technology (IT) related to Information Security, Software Testing/Certification and Development of National Level Assurance Framework in IT and software sectors through countrywide network of laboratories and centres. They are one of the Registered Certifying Bodies (RCBs) for various International Standards.

STQC laboratories have national/International accreditation and recognition's in the area of testing and calibration. In the area of IT & e-Governance, STQC offers quality assurance services as per National and International standards to the industry. More details on the functions of STQC can be accessed at <http://www.stqc.gov.in>.

#### **4.6 Practices in Television Broadcasting for Standardization, Certification and Accreditation**

There are different framework and standards that are used globally for creating and administering television broadcast standards. Some of the major standards are listed below:

1. European Standards
2. Digital Video Broadcast (DVB) Standards
3. Integrated Services Digital Broadcasting (ISDB) Standards
4. Advanced Television Systems Committee (ATSC) Standards
5. MovieLabs ECP Specifications

**4.7** Structure and process of European Standards Organization is similar to BIS. However, all the other standards like DVB, ATSC and ISDB are made by industry consortium/ Associations. For example, DVB project is an

international industry consortium that develops international open standards for digital television broadcast and receivers. More details of the process of establishing the standards, testing and certification process by these consortium / agencies are provided in **Annexure III**.

#### **4.8 Development of Indian Standards for Content Security in Digital Addressable Systems**

- 4.8.1 As discussed in previous chapters there is an absence of an overarching regulatory framework for standardization, testing and certification of CAS and SMS deployed in India. Although Schedule III of the Interconnection Regulations 2017 sets out a macro level framework, it only provides for the minimum requirements to be fulfilled by digital addressable systems. Since the criteria laid out in Schedule III are generic in nature, it does not control deployment of sub-standard solutions which are vulnerable to hacking, thereby putting content security at risk.
- 4.8.2 The extant regulatory framework vide Schedule III, only ensures conformity with Regulations, under the provisions of Audit of the DPO systems that entail testing of the relevant features, whereby if in the opinion of a broadcaster the addressable system being used by the distributor does not meet requirements specified in the Schedule III, he is permitted to disconnect signals of television channels, as per proviso to Sub-Regulation (2) of Regulation 15. There is no regulatory requirement for checking conformity to Indian Standards. However, this does not protect the interest of small MSOs who has installed sub-standard CAS and SMS due to lack of technical knowledge.
- 4.8.3 There is an absence of an overarching regulatory framework for standardization, testing and certification of conditional access systems deployed by distributors. CAS and SMS are pivotal for the Digital Addressable Broadcast eco-system and are responsible for delivery of the content in a secure & encrypted manner only to authorized subscribers.



Hence, there is an immediate need for drafting and deployment of adequate standards for content security for conditional access systems.

4.8.4 Existing Digital Video Broadcasting (DVB) standards are already an industry accepted standard for unidirectional broadcast for sending digital TV programs over satellite, cable, and terrestrial networks, as is evidenced by its wide adoption by all major technology vendors. Under the DVB standard, conditional access system (CAS) standards are defined in the specification documents for DVB-CA (conditional access), DVB-CSA (the common scrambling algorithm) and DVB-CI (the Common Interface). However, these standards only define a method by which one can obfuscate a digital-television stream, but the contents of ECMs and EMMs are not standardized and as such they depend on the conditional access system being used, which as discussed earlier, are proprietary in nature.

4.8.5 In addition to conformity with DVB Standards, major CAS vendors in India also comply with MovieLabs Enhanced Content Protection specification for new deployments and undergo Cartesian Robustness Tests in order to license premium UHD content from production studios. These specifications have been developed by a consortium of major Hollywood studios. Though, these are not statutory standards, but they've become de-facto standard for premium content protection in the industry.

4.8.6 Apart from industry driven standards, Bureau of Standards (BIS), is also in the process of formulation of standards for conditional access system (CAS). In BIS, the Audio, Video, Multimedia Systems and Equipment Sectional Committee, LITD 07 is responsible for preparation of Indian Standards relating to:

- a) Audio, video and multimedia systems and equipment and
- b) Acoustics, electroacoustic and related instruments.

LITD 07 Sectional Committee has representation from relevant ministries of the Government, TRAI, CDAC, STQC, major distribution platforms,

major CAS vendors, chip manufacturers, device manufacturers and academicians. Presently LITD 07 Sectional Committee in collaboration with all its members is in the process of developing draft standards for security testing of conditional access system (CAS). Presently, an ad-hoc group consisting of the operators, chip manufacturers, concerned ministries and organizations of the Government has been formed to further deliberate on the need, title, scope and roadmap for this draft standard.

- 4.9** In view of the above, it is evident that establishing recognized standards, certification, accreditation and testing procedures can be done in a number of ways. It can be industry driven where specialized agency(ies) can develop and publish standards in their domain areas. Subsequently, underlying provisions can be incorporated in requisite licensing and regulatory framework.
- 4.10** Another option exists where the Licensor (MIB in India) or the Regulator (TRAI) can formulate and issue the technical compliance framework. The framework may be developed through their own consultative processes or, by adopting/ incorporating relevant Indian/ International standards. In such case the task of effective oversight and implementation may also be performed as per license/ regulatory conditions. Regulator/ Licensor in the process will have to ensure that the technical framework is developed with the support and involvement of industry stakeholders. Such involvement can happen through structured committees or through wider stakeholder consultations. 'Technical Criteria' should be formulated in a transparent manner through a consensus process by the committees comprising of experts from all concerned areas such as technology vendors, producers/ manufacturers of devices, R&D centers, regulatory bodies etc.
- 4.11** In case the framework is defined by the licensor/ regulator, there will be a case for conducting the testing of systems for conformity of such standards.

There are independent accredited labs that can help in establishing such conformity tests and issuing relevant certification. In such a scenario, licensor/ regulator may authorize/ empanel organizations such as Broadcasting Consultants India Limited (BECIL) to conduct tests that establish conformity of CAS/ SMS systems to such license condition/ regulatory provisions.

**4.12** Alternatively, the technical framework for Content Security in Digital Addressable Systems can be developed by an independent agency/ industrial body or standards organization. Conformity assessment for compliance to such framework/ standards may be entrusted with existing certification agencies like BIS, STQC Directorate, QCI etc. Such assessment may include product testing, product certification and conformity to quality management systems etc.

**4.13** Apropos discussions in the above sections, the issues for consultation are:

**Q5. a) Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons thereof. Describe the structure and functioning procedure of such entrusted entity.**

**(b) What should be the mechanism/ structure, so as to ensure that stakeholders engage actively in the decision making process for making test specifications / procedures? Support your response with any existing model adapted in India or globally.**

**Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.**

**a) Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or**

**alternatively should the work of testing and certification be entrusted with accredited testing labs empanelled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.**

**(b) What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation?**

**(c) What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national/ international best practices.**

- Q7. Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?**
- Q8. Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end- consumer experience? Kindly provide detailed comments.**
- Q9. Any other issue relevant to the present consultation.**

## **CHAPTER 5**

### **ISSUES FOR CONSULTATION**

**Q1. List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?**

**Q2. As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?**

**Q3. Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?**

**Q4. What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?**

**Q5. a) Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons thereof. Describe the structure and functioning procedure of such entrusted entity.**

**(b) What should be the mechanism/ structure, so as to ensure that stakeholders engage actively in the decision making process for making test specifications / procedures? Support your response with any existing model adapted in India or globally.**

**Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.**

**a) Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of testing and certification be entrusted with accredited testing labs empanelled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.**

**(b) What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation?**

**(c) What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national/ international best practices.**

**Q7. Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?**

**Q8. Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end- consumer experience? Kindly provide detailed comments.**

**Q9. Any other issue relevant to the present consultation.**

## **List of Abbreviations**

<b>Abbreviations</b>	<b>Description</b>
API	Application Programming Interface
BIS	Bureau of Indian Standards
CAM	Conditional Access Module
CAS	Conditional Access System
CATV	Community Antenna Television
C-DOT	Centre for Development of Telematics
CI	Common Interface
CPE	Customer Premises Equipment
CW	Control Word
DAS	Digital Addressable System
DPO	Distribution Platform Operator
DRM	Digital Rights Management
DTH	Direct to Home
DVB	Digital Video Broadcasting
DVB-C	Digital Video Broadcasting - Cable
DVB-CSA	Digital Video Broadcasting-Common Scrambling Algorithm
DVB-S	Digital Video Broadcasting - Satellite



DVB-T	Digital Video Broadcasting - Terrestrial
ECI	Embedded Common Interface
ECM	Entitlement Control Message
EEE	Electrical and Electronic Equipment
EIT	Event Information Table
EMM	Entitlement Management Message
EPG	Electronic Program Guide
ETSI	European Telecommunications Standards Institute
HITS	Head End In the Sky
iDTV	Integrated Digital Television
ILA	Industry Licensing Authority
IPTV	Internet Protocol TV
ITU	International Telecommunications Union
LCOs	Local Cable Operators
LNBC	Low Noise Block Downconverter
MHP	Multimedia Home Platform
MIB	Ministry of Information and Broadcasting
MK	Master Key
MSOs	Multi-System Operators

OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OTA	Over-the-Air
OTT	Over-the-Top
PCMCIA	Personal Computer Memory Card International Association
QAM	Quadrature Amplitude Modulation
QoS	Quality of Services
QPSK	Quadrature Phase Shift Keying
SC	Smart Card
SCK	Secret Chipset Key
SDN	Software Defined Networks
SK	Service Key
SoC	System on Chip
STB	Set-Top Box
TA	Trusted Authority
TDSAT	Telecom Disputes Settlement and Appellate Tribunal
UHF	Ultra-High Frequency
VHF	Very High Frequency

**Annexure I**  
**(Chapter no. 1/Para no. 1.8)**

**“Schedule III**

*(Refer sub-regulation (6) of the regulation 10 and regulation 15)*

**Scope and Scheduling of Audit**

- (A) Scope: The annual Audit caused by Distributor shall include the Audit to validate compliance with this Schedule and the Subscription Audit, as provided for in these regulations.
- (B) Scheduling: The annual Audit as caused by Distributor under regulation 15 (1) shall be scheduled in such a manner that there is a gap of at-least six months between the audits of two consecutive calendar years. Further, there should not be a gap of more than 18 months between audits of two consecutive calendar years.

**Addressable Systems Requirements**

**(C) Conditional Access System (CAS) and Subscriber Management System (SMS):**

1. The distributor of television channels shall ensure that the current version of the CAS, in use, do not have any history of hacking.  
*Explanation:* A written declaration available with the distributor from the CAS vendor, in this regard, shall be construed as compliance of this requirement.
2. The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.
3. It shall not be possible to alter the data and logs recorded in the CAS and the SMS.
4. The distributor of television channels shall validate that the CAS, in use, do not have facility to activate and deactivate a Set Top Box (STB) directly from the CAS terminal. All activation and deactivation of STBs shall be done with the commands of the SMS.
5. The SMS and the CAS should be integrated in such a manner that activation and deactivation of STB happen simultaneously in both the systems.  
*Explanation:* Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the SMS and the CAS terminals.
6. The distributor of television channels shall validate that the CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded.
7. The fingerprinting should not get invalidated by use of any device or software.
8. The CAS and the SMS should be able to activate or deactivate services or STBs of at least Five percent (5%) of the subscriber base of the distributor within 24 hours.
9. The STB and Viewing Card (VC) shall be paired from the SMS to ensure security of the channel.
10. The CAS and SMS should be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB by STB basis.

11. The SMS should be computerized and capable of recording the vital information and data concerning the subscribers such as:
  - (a) Unique customer identification (ID)
  - (b) Subscription contract number
  - (c) Name of the subscriber
  - (d) Billing address
  - (e) Installation address
  - (f) Landline telephone number
  - (g) Mobile telephone number
  - (h) E-mail address
  - (i) Channels, bouquets and services subscribed
  - (j) Unique STB number
  - (k) Unique VC number.
12. The SMS should be capable of:
  - (a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs.
  - (b) Locating each and every STB and VC installed.
  - (c) Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.
13. The SMS should be capable of generating reports, at any desired time about:
  - (a) The total number of registered subscribers.
  - (b) The total number of active subscribers.
  - (c) The total number of temporary suspended subscribers.
  - (d) The total number of deactivated subscribers.
  - (e) List of blacklisted STBs in the system.
  - (f) Channel and bouquet wise monthly subscription report in the prescribed format.
  - (g) The names of the channels forming part of each bouquet.
  - (h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time.
  - (i) The name of a-la carte channel and bouquet subscribed by a subscriber.
  - (j) The ageing report for subscription of a particular channel or bouquet.
14. The CAS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the CAS including but not limited to activation and deactivation commands issued by the SMS.
15. The CAS shall be able to tag and blacklist VC numbers and STB numbers that have been involved in piracy in the past to ensure that such VC or the STB cannot be re-deployed.
16. It shall be possible to generate the following reports from the logs of the CAS:
  - (a) STB-VC Pairing / De-Pairing
  - (b) STB Activation / De-activation
  - (c) Channels Assignment to STB
  - (d) Report of the activations or the deactivations of a particular channel for a given period.
17. The SMS shall be capable of generating bills for each subscriber with itemized details such as the number of channels subscribed, the network capacity fee for the channels subscribed, the rental amount for the customer premises equipment, charges for pay channel and

bouquet of pay channels along with the list and retail price of corresponding pay channels and bouquet of pay channels, taxes etc.

18. The distributor shall ensure that the CAS and SMS vendors have the technical capability in India to maintain the systems on 24x7 basis throughout the year.
19. The distributor of television channels shall declare the details of the CAS and the SMS deployed for distribution of channels. In case of deployment of any additional CAS/ SMS, the same should be notified to the broadcasters by the distributor.
20. Upon deactivation of any subscriber from the SMS, all programme/ services shall be denied to that subscriber.
21. The distributor of television channels shall preserve unedited data of the CAS and the SMS for at least two years.

**(D) Fingerprinting: -**

1. The distributor of television channels shall ensure that it has systems, processes and controls in place to run finger printing at regular intervals.
2. The STB should support both visible and covert types of finger printing. Provided that only the STB deployed after coming into effect of these Amendment regulations shall support the covert finger printing.
3. The fingerprinting should not get invalidated by use of any device or software.
4. The finger printing should not be removable by pressing any key on the remote of STB.
5. The finger printing should be on the top most layer of the video.
6. The finger printing should be such that it can identify the unique STB number or the unique VC number.
7. The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), Settings, blank screen, and games etc.
8. The location, font colour and background colour of fingerprint should be changeable from head end and should be random on the viewing device.
9. The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the VC.
10. The finger printing should be possible on global as well as on the individual STB basis.
11. The overt finger printing should be displayed by the distributor of television channels without any alteration with regard to the time, location, duration and frequency.
12. Scroll messaging should be only available in the lower part of the screen.
13. The STB should have a provision that finger printing is never disabled.
14. The watermarking network logo for all pay channels shall be inserted at encoder end only. Provided that only the encoders deployed after coming into effect of these Amendment regulations shall support watermarking network logo for all pay channels at the encoder end.






**(E) Set Top Box (STB): -**

1. All STBs should have a Conditional Access System.
2. The STB should be capable of decrypting the Conditional Access messages inserted by the Head-end




3. The STB should be capable of doing finger printing. The STB should support both Entitlement Control Message (ECM) and Entitlement Management Message (EMM) based fingerprinting.
4. The STB should be individually addressable from the Head-end.
5. The STB should be able to receive messages from the Head-end.
6. The messaging character length should be minimal 120 characters.
7. There should be provision for global messaging, group messaging and the individual STB messaging.
8. The STB should have forced messaging capability including forced finger printing display.
9. The STB must be compliant to the applicable Bureau of Indian Standards.
10. The STBs should be addressable over the air to facilitate OTA software upgrade.
11. The STBs with facilities for recording the programs shall have a copy protection system.

## Annexure II (Chapter no. 3/Para no. 3.4.11)





### Standard Vs Sub-standard CAS



S No.	Area / Subject	Risk Factor/ Criticality	Standard CAS	Sub Standard CAS	Risk/ Area affected
1	Control Word (CW)	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. It has protection against CW sharing.</li> <li>2. CW is sent in an encrypted format in the Entitlement Control Message (ECM) in it.</li> <li>3. It is not possible to get the CW by snooping methods in it.</li> </ol>	<ol style="list-style-type: none"> <li>1. It does not have any protection against CW Sharing</li> <li>2. CW is not sent in an encrypted format in the Entitlement Control Message (ECM) in it.</li> <li>3. It is possible to get the CW by snooping methods in it.</li> </ol>	If CW is not protected, then it would allow the Local Cable Operator (LCO)/ Hacker/ to redistribute the signals without the knowledge of the Operator / Broadcaster and get profited from it.
2	Entitlement Control Message (ECM)  Entitlement Management Message (EMM)	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. ECM and EMM are encrypted in Standard CAS</li> <li>2. It is not possible to get the ECM and EMM by snooping methods in it</li> <li>3. It has mechanism for Custom EMM generation and handling.</li> </ol>	<ol style="list-style-type: none"> <li>1. ECM and EMM are not encrypted in Sub Standard CAS</li> <li>2. It is possible to get the ECM and EMM by snooping methods in it</li> <li>3. It does not have mechanism for Custom EMM generation and handling.</li> </ol>	If ECM / EMM are not protected, then it would allow the Local Cable Operator (LCO) / Hacker/ to redistribute the signals without the knowledge of the Operator / Broadcaster and get profited from it. Lack of flexibility for custom EMM generation and handling poses security risk if the original EMM generation mechanism is broken.
3	Piracy Control	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. It has piracy control by using various types of Finger Printing Mechanisms</li> </ol>	<ol style="list-style-type: none"> <li>1. It does not have piracy controls by using various types of Finger Printing Mechanisms</li> </ol>	Content can be pirated and redistributed on various online as well as offline mechanisms without the knowledge of the operator or the broadcaster
4	Key Ladder	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. It supports Hardware Key Ladder within the System on Chip (SoC)</li> </ol>	<ol style="list-style-type: none"> <li>1. It does not support hardware key ladder within the System on Chip (SoC)</li> </ol>	Content Piracy and Redistribution without the knowledge and permission of the broadcaster and the operator
5	Descrambling	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. It supports Hardware Descrambling within the System on Chip (SoC)</li> </ol>	<ol style="list-style-type: none"> <li>1. It does not support hardware Descrambling within the System on Chip (SoC)</li> </ol>	Content Piracy and Redistribution without the knowledge and permission of the broadcaster and the



6	Auto Expiry	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. In standard CAS the Set Top Box (STB) gets de-entitled to the services automatically on the expiry date set at the beginning of the subscription period and does not need a command from the Subscriber Management System (SMS) to get de-entitled</li> </ol>	<ol style="list-style-type: none"> <li>1. In Sub- Standard CAS the Set Top Box (STB) does not gets de-entitled to the services automatically on the expiry date set at the beginning of the subscription period and needs a command from the Subscriber Management System (SMS) to get de-entitled</li> </ol>	operator Sub Standard CAS increases the traffic of the SMS commands to send entitlement and de-entitlement commands every month for every customer. It results in huge bandwidth consumption if the network has few thousand customers and few hundred services and packages to subscribe.
7	Boot Loader	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. Standard CAS has secure boot loader which allows only authenticated software to boot up the STB.</li> <li>2. Standard CAS has Secure boot loader which provides protection against the malicious software download in an STB.</li> </ol>	<ol style="list-style-type: none"> <li>1. Sub - Standard CAS does not have secure boot loader and hence it allows non-authenticated software to boot up the STB.</li> <li>2. Sub Standard CAS does not have Secure boot loader which allows the malicious software download in an STB.</li> </ol>	<p>Non Secure Boot Loader can put investment of the operator on the STB at risk because if a malicious software is run on the STB it can make the boxes to behave abnormally and can even make all the STBs dead / stop working completely making the operator to re-invest in buying all the boxes once again.</p> <p>Non-Secure Boot loader can also compromise in releasing the control word which would allow the end user to redistribute the signals without the knowledge of the Operator / Broadcaster</p>
8	Addressability	Very High & Very Critical 	<ol style="list-style-type: none"> <li>1. In Standard CAS the EMM addressability in individual/ groups/region / global / LCO is achievable. The definition of the groups may be based on rules definitions such as geographic locations based on pin code, city, etc.</li> </ol>	<ol style="list-style-type: none"> <li>1. In Sub - Standard CAS the EMM addressability in individuals / groups/ region/ global / LCO is not achievable. The definition of the groups may not be based on rules definitions such as geographic locations based on pin code, city, etc.</li> </ol>	<p>Sub Standard CAS denounces the very purpose of the Government of India DAS (Digital Addressable System) program and its guidelines. This results in various indirect losses of revenue and content piracy.</p> <p>The operator and broadcaster lose the control on the field</p>



					network and its STBs.  It also increases the workload of the operator.
9	Blacklisting	Very High & Very Critical 	1. Standard CAS has provision for blacklisting of smart cards or ID's of the STBs	1. Sub Standard CAS does not have a provision for blacklisting of smart cards or ID's of the STBs	Sub Standard CAS allows compromised STBs to continue to run in the network thereby allowing content piracy to continue without the knowledge of the operator or the broadcaster.
10	B Mails / Alerts	High & Critical 	1. Standard CAS supports B Mails / Alerts which may be typed (persistent, one-time, viewable, stored-until-deleted etc.)	1. Sub - Standard CAS does supports B Mails / Alerts which may be typed (persistent, one-time, viewable, stored-until-deleted etc.)	Sub Standard CAS makes difficult to send message to end user which may be critical to continue the service or inform the end user of some life-threatening disaster / calamity etc.
11	Message Queue	High & Critical 	1. In Standard CAS the head-end queues up the messages in case of non-successful transmission of messages due to STB not powered on or network element failures and retries them at specified intervals using additive back off retrial timings. The life of the messages in case there are unsuccessful deliveries are specifiable.	1. In Sub Standard CAS the head-end does not queues up the messages in case of non-successful transmission of messages due to STB not powered on or network element failures and does not retries them at specified intervals using additive back off retrial timings. The life of the messages in case there are unsuccessful deliveries are not specifiable.	Sub Standard CAS increases the workload of the operator and creates a confusion among the end consumers who start getting non uniform services from the same operator  It also increases the Bandwidth of the messaging signals thereby increasing the cost of operations for the service operators.
12	CAS Reports & Data Base	Very High & Very Critical 	1. Standard CAS generates reports in Non-Editable Format only like pdf  2. Standard CAS provides correct, genuine and authentic data  3. Standard CAS does not have any backdoors to manipulate the data by the operators	1. Sub Standard CAS generates reports in Editable Formats also like csv, excel  2. Sub Standard CAS does not provide correct, genuine and authentic data  3. Sub Standard CAS has backdoors to manipulate the data by	Sub Standard CAS / SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the operator, broadcaster as well as to the government in form of taxes.

			<p>4. Standard CAS generates logs which are not accessible by any user for manipulation and/ or modification.</p> <p>5. The Standard CAS ensure that it has option to back up all the critical data as per the configuration.</p>	<p>the operators</p> <p>4. Sub Standard CAS generates logs which are accessible by any user for manipulation and/ or modification.</p> <p>5. The Sub-Standard CAS / do not have an option to back up all the critical data as per the configuration.</p>	
13	CAS Server Hardware	<p>High &amp; Very Critical</p> 	<p>1. Standard CAS are deployed on hardened server hardware specifically supplied by CAS provider and it is not possible to deploy standard CAS in just any commercially available generic servers thereby providing extra layer of data / cyber security and removing the probability of any backdoors and malicious software deployments.</p>	<p>1. Sub Standard CAS are not deployed on hardened server hardware specifically supplied by CAS provider and it is possible to deploy sub-standard CAS in just any commercially available generic servers thereby removing any extra layer of data / cyber security and increasing the probability of any backdoors and malicious software deployments.</p>	<p>Having backdoors in the system may result into potential sabotage by interested parties to take over network and compromise it by sending unlawful and vicious messages to masses/ communities thereby disturbing the socio-cultural fabric of the society / country at large.</p> <p>It can also result into content theft/ piracy / revenue loss for all eco system partners.</p>
14	Audit and Certification by Globally Recognized Third Party Content Security Auditors/ Labs	<p>High &amp; Critical</p> 	<p>1. A Standard CAS is audited and certified by globally recognized Third Party Content Security experts and is rated based on the scores provided by them in an unbiased manner. Such 3<sup>rd</sup> parties include – Cartesian/ Farncombe / NIST USA / Atsec / Riscure / Rambus etc.</p>	<p>1. A Sub-Standard CAS is not audited and not certified by any globally recognized Third Party Content Security experts and does not have any ratings.</p>	<p>Since CAS is based on certain proprietary mechanisms for obfuscation and security, a non-certified Sub-standard CAS results in not providing a complete control and visibility to either the statutory / regulatory bodies of the country or the broadcaster / operator because of which the end user sometimes is deprived of the best content as well as the risk of revenue loss and content piracy is increased significantly.</p>



**International Experience Standards, Testing and Certification  
for Digital Television Broadcasting**

**i) European Standards:**

European Standards Organizations (ESOs) support European regulations and legislation through the creation of harmonized European Standards dealing with telecommunications, broadcasting and other electronic communications networks and services. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as the European Standards (ENs).

The EC (European Commission)/ EFTA (European Free Trade Association (EFTA) issues standardization requests to ETSI, CEN and CENELEC, with proposals to develop Harmonized Standards (European Standards (ENs) with a special status). The ESOs agree together whether and how they want to respond to a specific standardization request, for example, which of the ESOs will carry out or lead the work. These Harmonized Standards provide the technical detail necessary to achieve the 'essential requirements' of a Directive. By adhering to these harmonized standards, manufacturers and service providers can demonstrate that they have followed the essential requirements of the directive and are able to claim 'presumption of conformity'. This allows them to put their products and services on the market in Europe. All Member States of the European Union must allow a product to be placed on the market and used in their territories if it complies with the relevant Directives<sup>15</sup>.

**ii) DVB Standards:**

DVB Project is an international industry consortium that develops DVB standards as a set of international open standards for digital television. DVB

---

<sup>15</sup> <https://www.cencenelec.eu/standards/ESOs/Pages/default.aspx>

specifications are standardized in one of the European statutory standardization bodies i.e. European Telecommunications Standards Institute (ETSI), European Committee for Electrotechnical Standardization (CENELEC) and European Broadcasting Union (EBU) and are subsequently published by a Joint Technical Committee (JTC) of these bodies.

The DVB-S system is used across the world, though in some countries such as Japan and the United States other digital satellite systems are used as well as DVB-S. The DVB-C system is also widely used throughout the world. The DVB-T system is the least widely used, though the roll out of digital terrestrial television throughout the world has been slower than digital satellite and cable. CAS for DVB can be implemented as SimulCrypt and MultiCrypt. It uses DVB Common Scrambling Algorithm (DVB-CSA) or AES-128 (mandatory for devices). It is estimated that nearly 1 Billion DVB receivers have been deployed around the world.

### **iii) Integrated Services Digital Broadcasting (ISDB) Standards**

ISDB is a Japanese standard for digital television (DTV) and digital radio maintained by the Japanese organization ARIB (Association of Radio Industries and Businesses).<sup>16</sup> ARIB is a standardization organization in Japan whose members include telecommunication companies, broadcast companies, R&D companies, banks and infrastructure agencies.

Presently, many countries, including a number of Central and South American nations have adopted ISDB over other digital broadcasting standards. The core standards of ISDB are ISDB-S (satellite television), ISDB-T (terrestrial), ISDB-C (cable) and 2.6 GHz band mobile broadcasting.

CAS specifications for ISDB systems are defined in ARIB STD-B25. ARIB STD-B25 defines the control system for reception (Conditional Access System) and control for playback (Conditional Playback System) used in ISDB system. Main parameters of ARIB STD-B25 system are defined in Recommendation ITU-R

---

<sup>16</sup> <https://www.arib.or.jp/english/index.html>

BT.1852. CAS for ISDB is referred to as CAS-R system. This system uses cipher for scrambler and descrambler based on MULTI2 (ISO/IEC 9979). The second-generation CAS is also specified in ARIB STD-B61.

#### **iv) Advanced Television Systems Committee (ATSC) Standards**

They are a set of standards for digital television transmission over terrestrial, cable, and satellite networks used mostly in the United States, Mexico and Canada. They were developed in the early 1990s by the Grand Alliance, consortium of electronics and telecommunications companies. The standard is now administered by the Advanced Television Systems Committee. ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

ATSC coexists with the DVB-T standard, and with ISDB-T (Japanese standard for Digital TV). A similar standard called ADTB-T was developed for use as part of China's new DMB-T/H dual standard. CAS specifications for ATSC Terrestrial Broadcasting are defined in ATSC Standard A/70 Part 1. This standard defines building blocks (Simulcrypt, Common scrambling, Host CA Software, Return Channel, and CA Module Interface) necessary to ensure interoperability. Method for utilizing Simulcrypt concepts are given in ATSC Standard A/70 Part 2. Content Protection and Content Management for the ATSC environment is addressed in Standard A/98, "System Renewability Message Transport"

In US, digital broadcasts when transmitted as over-the-air signals must conform to ATSC standards. These standards define, format and transmission criteria that ensure consistency, accessibility, and fairness for consumers and equipment manufacturers alike in the U.S., as well as international compatibility.

#### **v) MovieLabs ECP Specifications**

MovieLabs is an independent non-profit organization founded by the six major Hollywood studios to advance research and development in motion picture distribution and protection. In 2013, they published v1.0 of the MovieLabs Enhanced Content Protection Specification. This specification describes a set of high-level security requirements for the distribution of Hollywood UHD content to consumer devices. Technologies aiming to support UHD content must be compliant with ECP.

ECP Specifications act as a guide for companies interested in developing secure products. Each MovieLabs member company decides independently the extent to which it utilizes, or requires adherence to, these specifications. However, failure to meet the ECP requirements may generally mean that service providers cannot license UHD content from Hollywood studios. The specification has been updated twice since it was first published — v1.1 was released in February 2015, and a more recent update produced v1.2 in August 2018.<sup>17</sup>

Although targeted at UHD content, the ECP specification describes best practice for many premium content services, including Pay TV and live sports. ECP represents the de-facto standard for content protection in the industry and ECP compliance is generally considered mandatory for any new service aiming to carry premium content (including non-UHD services). The MovieLabs ECP specification documents the security needs of the Hollywood studios. Compliance of these specifications is ensured by third-party audits such as Farncombe Security Audit. The Farncombe Security Audit is recognized by studios and sports right holders worldwide as a measure of a solution's suitability to protect premium content. They have established a set of Minimum-Security Requirements that are compiled and maintained through dialogue with content owners and technology partners.

---

<sup>17</sup> [https://movielabs.com/ngvideo/MovieLabs\\_ECP\\_Spec\\_v1.2.pdf](https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf)