Pay Television

Best regulatory practices to combat fraud of subscription-based television signals

OAS | CITEL | ALIANZA CONTRA LA PIRATERÍA DE TELEVISIÓN PAGA

Pay Television

Best regulatory practices to combat fraud of subscription-based television signals

OAS CITEL

ALIANZA
CONTRA LA PIRATERÍA DE TELEVISIÓN PAGA

This Manual has been prepared by mandate of the Permanent Consultative Committee I: Telecommunications/ ICTs of the Inter-American Telecommunication Commission in compliance with Resolution PCC.I/RES. 242 (XXVI-15). The Drafting Group was coordinated by the Administration of Uruguay.

We wish to thank the Alliance Against Pay-TV Piracy for their information and contributions to this manual.

Prepared and published by the Inter-American Telecommunications Commission (CITEL)

CITEL

Inter-American Telecommunication Commission

Organization of American States (OAS)

Permanent Consultative Committee I: Telecommunications/
Information and Communication Technologies (PCC.I)

1889 F St. NW

Washington, DC, Unites States of America

www.citel.oas.org

Executive Secretariat of CITEL
Phone: +1 202 370 4713
Fax: +1 202 458 6854

E-mail: citel@oas.org

June, 2017

Foreword

Currently, fraud linked to subscription-based satellite television signals represents a significant percentage with respect to the different forms of fraud in the consumption of audiovisual content. This affects both the industry producing audiovisual content as well as the entire industrial chain, from generating the content to making it available for public consumption in general; at the same time, it damages and negatively impacts the implementation of policies that promote local content developments and distribution.

This type of fraud and its implications are one of the aspects which, in the case of Uruguay, have driven the development and implementation of legislation prohibiting the manufacture, importation, sale, rental, and circulation of unauthorized subscription-based satellite television receivers. Regulations include banning entry into the country of any satellite television receiver without due authorization from the URSEC, the government body responsible, inter alia, for the supervision and verification of communications and audiovisual communication services.

In response to this problem, the National Directorate of Telecommunications of the Uruguayan Ministry of Industry, Energy and Mining, proposed and coordinated, within the framework of the Rapporteurship on Fraud Control, Regulatory Non-compliance Practices in Telecommunications and Regional Measures against the Theft of Mobile Terminal Devic-

es of the Working Group on Policy and Regulation of the Inter-American Telecommunication Commission (CITEL) of the Organization of American States (OAS), and, together with the international organization Alliance Against Pay-TV Piracy, the creation of this manual, which contains a set of best regulatory practices to combat the manufacture, importation, rental, marketing and/or distribution of satellite receivers capable of decrypting subscription-based satellite television signals without proper authorization, or that can be modified for this purpose.

We hope that this material will serve as an informative contribution, and to help encourage the implementation of measures to combat this type of fraud in those Member States of the OAS, represented by their Telecommunications Authorities that deem it necessary.

Nicolas Antoniello
National Directorate of
Telecommunications, Ministry
of Industry, Energy and Mining,
Oriental Republic of Uruguay

Foreword

Pay TV fraud represents a threat to intellectual property rights, and significantly affects the development of the audiovisual industry as well as the economy of the countries of the Americas. For this reason, it is essential to raise awareness on this issue, develop policies that control it, and establish strategies to combat this form of fraud. In its different forms, estimated pay TV fraud volumes range from 12% in regions with less fraud to more than 40% in the regions most affected by the different forms of fraud. These modalities include online audiovisual content fraud, and illegal signal retransmission through illegal decoders. The lower revenue received by the audiovisual industry entail lower income for the Member States of the OAS, particularly regarding tax matters. The people of the Americas deserve to enjoy the wide variety of audiovisual content that are available for consumption, both in traditional and online formats, which requires an adequate protection of intellectual property.

The exchange of experiences and best practices between the Member States of the OAS facing these types of fraud will help make more effective the work of legislating, identifying gaps, and addressing the challenges and losses that this illegal activity represents.

Oscar León
Executive Secretary General
Inter-American Telecommunication
Commission (CITEL)
Organization of American States

Contents

Executive Summary

Since it emerged in the early 1990s, the service of subscription satellite television (TV), also called pay satellite TV, has experienced rapid growth in the Americas, reaching more than 86 million homes in the fourth quarter of 2016.[1] The number of pay satellite TV subscribers in Latin America has grown from 18 million in 2011 to more than 50 million in 2016, representing a compound annual growth rate (CAGR) of 23%.[2] If this growth rate continues, it is estimated that, by the end of 2020, Latin America will reach more than 70 million pay satellite TV subscribers.

Likewise, pay satellite TV has become an alternative to reach remote regions (which are difficult to access by terrestrial broadcast television due to the geographical diversity of Latin America) with audiovisual content and plans with innovative payment options, fulfilling the social objective of informing and entertaining rural populations.

The population of Latin America has benefited not only in terms of the coverage of audiovisual content through satellite TV, but also from higher levels of competition in the subscription TV market, with more choices of content and offers.

However, in recent years the sale of satellite receivers that illegally access satellite pay TV has spread in the Americas, posing a threat to the sector and putting its future development at risk, since the use of illegal receiver equipment has become a significant portion of total subscription TV fraud in Latin America.

The aim of this document, "Best regulatory practices to combat fraud of subscription-based television signals", is to highlight the problems in the Americas around the marketing and sale of receiver equipment that illegally access satellite pay TV. In this sense, the document describes the different modalities through which pay satellite TV is accessed illegally, review the regulatory progress made to combat this phenomenon in the Americas as well as international best practices, and to present recommendations that can be followed by the Governments in the region, in a harmonized way, to fight this type of fraud.

The technical recommendations for the Governments of the Americas to combat fraud of subscription-based television signals are:

» To develop a legal framework to fight against the manufacture, importation, distribution, rental, marketing, promotion, installation, circulation, and/or use of illegal devices.

» To develop a legal framework to punish the circumvention, evasion, disabling, and/or suppression of the technological security measures set up by the holders of subscription satellite TV signals and/or the holders of the contents of such signals.

» To focus more efforts on the control of those stages prior to the use of illegal devices by end users.

---

1 Data estimated by the Telecommunications Management Group, Inc., based on information published by the Business Bureau (Pay TV Market Estimates, December 2016), Leichtman Research Group (Research Notes, 3Q 2016), and the Federal Institute of Telecommunications of Mexico [Instituto Federal de Telecomunicaciones de México] (Statistical Report, 3Q 2016).

2 The following countries are included: Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, Puerto Rico, Uruguay, and Venezuela, as well as the countries/territories of the Caribbean, Aruba, Barbados, Curacao, and Trinidad y Tobago.

» Establish, as requisite for the entry of FTA (*free-to-air*) devices without the ability to decrypt signals from subscription satellite TV systems or that could be modified for this purpose, a framework of suitable controls that ensures their correct harmonization to restrict the import, distribution, sale, and circulation of these devices. For the purposes of control, and in view of the complexity of the technology involved, the relevant authorities may require the industry to cooperate in controlling the entry of the FTA devices in question, providing an independent specialized technical team to which the authorities can recur in order to determine such harmonization.

» To establish provisions to ensure that decoder devices with the ability to decrypt encoded signals may only be imported by authorized pay television operators whose license enables them to carry out such imports.

» Based on the attributes described in this report, to define the procedures that allow the identification of illegal devices.

» To develop a monitoring system that allows the traceability of satellite television receivers.

» To develop a system through which complaints can be channeled when fraudulent practices related to the manufacture, importation, rental, marketing, distribution, promotion, installation, circulation, and/or use of illegal devices are verified.

» To combat any commercial communications by any means that deal in the promotion of illicit devices.

» To establish a system of appropriate penalties when detecting non-compliance within the legal framework that is already applicable or to be implemented.

» To improve the performance and coordination of different State agencies and private operators involved in the aforementioned activities.

» To promote the harmonization of policies related to the control of this type of fraud among the Member States of CITEL.

Introduction

This manual presents a series of recommendations on best regulatory practices to combat the manufacture, importation, rental, marketing, distribution and/or use of receiver devices capable of decrypting subscription satellite television (TV) signals without due authorization, or those devices that can be modified to do so. The development of this manual is part of the mandate set out in the resolution of Permanent Consultative Committee I: Telecommunications / Information and Communication Technologies (PCC.I), Resolution PCC.I/RES. 242 (XXVI-15), of the Inter-American Telecommunication Commission (CITEL).

The manual contains currently adopted measures, recommendations and best practices from contributions made by the Member States and Associate Members of CITEL to PCC.I, in line with the aforementioned resolution.

The use of unauthorized satellite television signal receivers has been defined by Resolution PCC.I/RES. 242 (XXVI-15) as a type of fraud in the following way: "Satellite receiver devices with decryption capabilities to illegally access signals from satellite television systems without due authorization or which could be modified for that purpose".

This type of fraud and its corresponding definition has been included in the Classification Table on Fraud and Regulatory Practices in annexes 1 and 2 of Decision PCC.I/DEC. 204 (XXV-14).

Chapter 1 of this manual provides the description of subscription satellite television service and open (Free-To-Air) satellite television. In addition, it gives the definition of illegal devices used to decrypt subscription satellite television signals without proper authorization. Chapter 2 describes the main processes through which fraud is perpetrated when receiving subscription television signals by means of illegal devices, *i.e.*, *Internet Key Sharing* (IKS) and *Satellite Key Sharing* (SKS), and the attributes that must be validated to identify illicit devices. Chapter 3 summarizes the ten (10) responses received by the Member States to the questionnaire of Resolution PCC.I/RES. 242 (XXVI-15) including information reported by Member States in accordance with Recommendation PCC.II/REC. 45 (XXV-15). Nine (9) countries have confirmed they have implemented measures to combat the manufacture, importation, rental, marketing, distribution and/or use of satellite receiver devices capable of decrypting subscription satellite television (TV) signals. One (1) country mentions that it is currently studying measures to implement in the short term. Chapter 4 introduces best international practices, specifically in the European Union. Finally, Chapter 5 presents a series of recommendations to implement effective measures to efficiently combat fraud regarding the reception of subscription satellite television signals by means of illegal devices.

13

Chapter 1

Satellite television services

15

Satellite television services are divided into two categories: (i) subscription-based satellite television, and (ii) FTA (open) satellite television. The main difference between these services is the existence -or not- of an obligation to pay, either to rebroadcast or to access the audio and video content broadcast by the satellite system. This difference has important implications in the technical configuration, management, and security of satellite television content. This chapter describes the characteristics and operation of both service types.[3]

Subscription-based satellite television

Subscription-based satellite television service, also known as subscription satellite television, operates from a direct-to-home (DTH) system for the distribution of television signals broadcast directly to the public from geostationary satellites.

To guarantee the protection of the content being broadcast via satellite signals, DTH services use Conditional Access Systems or CAS. The purpose of CAS is to manage and protect the content of television broadcasters that are being distributed by the subscription television service provider, encrypting audio and video signals in order to avoid non-authorized access to said content.

Usually, to acquire pay television services, users must purchase or rent a decoder or *set-top-box* (STB) and an official smart card from the DTH service provider. Smart cards are used to manage and store the rights to decode content based on the service or programming package acquired by the subscriber.

CAS encrypts television signals and the content of DTH services by means of keys known as Control Words (CWs), which are constantly being updated (every few seconds) and transmitted through the network. DTH operators invest in cutting-edge technology to keep these keys periodically updated. The keys are received by the STB in order to decrypt the audio and video content when the subscriber wishes to watch a given signal.

CWs are encrypted in turn to avoid their interception and utilization by unauthorized third parties to access the protected content. To this effect, CWs are transmitted by means of encrypted packages called Entitlement Control Messages (ECMs), and the keys being encrypted by ECMs are called transmission keys. Transmission keys are stored in the memory of the smart cards included in the STB. DTH operators have the ability to change the transmission keys, as applicable, through administrator-level commands.

3 This chapter was prepared based on information provided by Nagra.

Figure 1: Operation of a subscription-based satellite television system
LNB: *Low Noise Block*, receives the signal from the satellite and amplifies it.

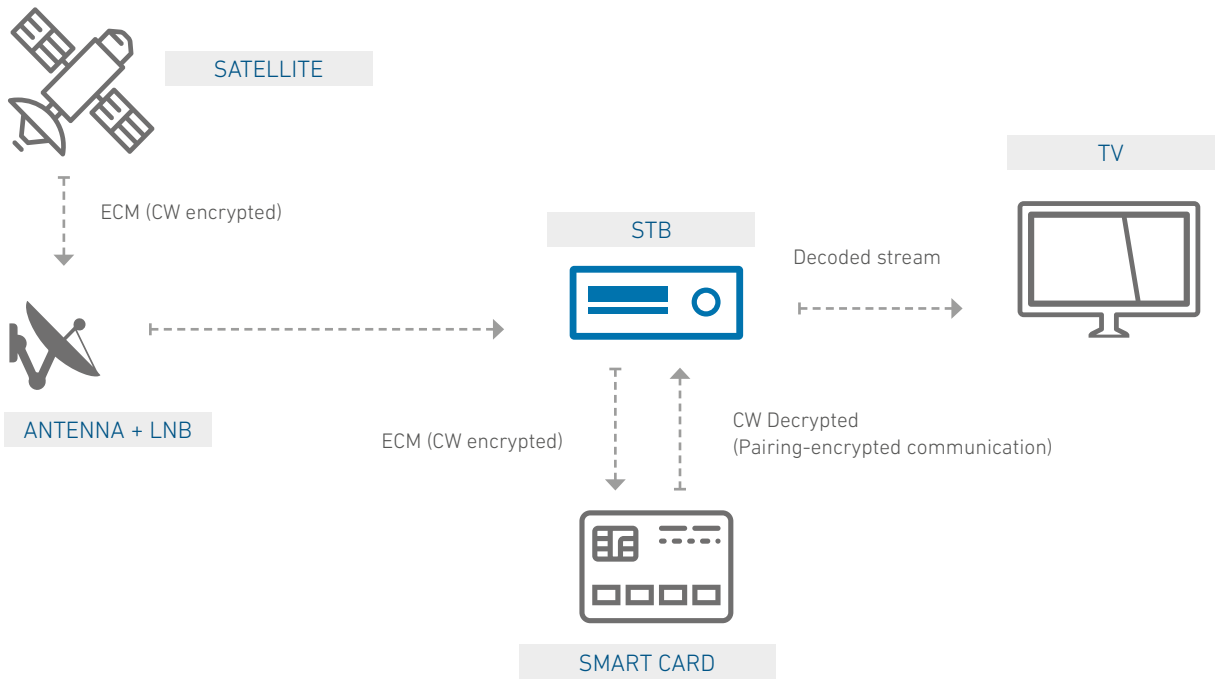
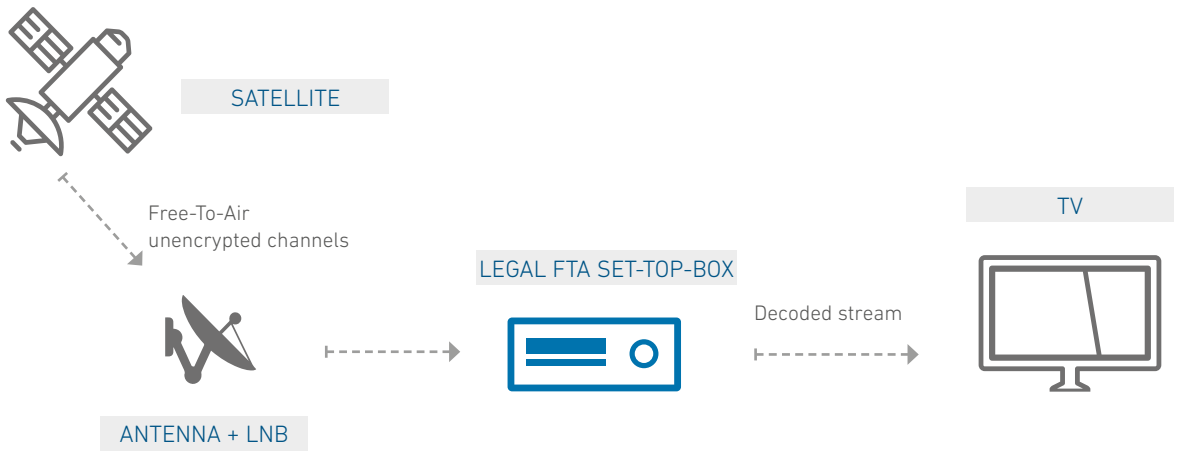


Figure 1 describes the process to receive content protected by the CAS. When a subscriber wants to watch a given signal, the STB receives an ECM from the DTH provider and sends it to the smart card. The smart card decrypts the ECM using the transmission key that is currently valid and then queries its database to find the rights assigned to the ECM to watch the signal in question (it determines if the subscriber has acquired the rights to see this specific signal). If the rights match, the smart card sends the CW to the STB. The CW must be encrypted again to protect the communication between the smart card and the STB. This process of protecting the satellite signal is called *pairing*.

Free-to-Air Satellite Television

Free-to-Air (FTA) Satellite Television services allow the reception of satellite signals that, by decision of the holder of the rights to that particular content, are broadcast with no encryption and thus are not protected by a CAS. Taking this into account, FTA content may be received and watched by any device connected to a satellite receiver. These decoding devices or STBs do not have the ability to decrypt signals, so they can only receive FTA signals. These devices are usually known as "FTA devices" by the industry (Figure 2).

Figure 2: Operation of an FTA device.
LNB: *Low Noise Block*, receives the signal from the satellite and amplifies it.



Illegal Devices

Illegal devices are those that have the ability to decrypt signals from subscription/based satellite television systems without due authorization or which could be modified for that purpose. These devices have been commonly sold under the label of “FTA devices”.

FTA devices are exclusively designed to allow the reception of unencrypted satellite signals or signals not protected by CAS (free content), whereas illicit devices allow illegal access to encrypted satellite signals.

Chapter 2

Reception of unauthorized satellite television signals

19

This chapter describes the main processes through which fraud is perpetrated when receiving subscription television signals by means of illegal devices.[4] In particular, the following two types of fraud are discussed:

» Sharing a key through a server that is accessible through the Internet, known as *Internet Key Sharing* (IKS).

» Sharing a key through a server that is accessible through an Internet satellite connection, known as *Satellite Key Sharing* (SKS).

IKS and SKS are currently the most widely used forms of fraud in Latin America. We will present, for each of these two types of fraud (IKS and SKS), the network topology, platforms and main components, as well as their functions. In addition, the attributes to identify illegal devices are included, which is essential to monitor the introduction, into the country, of devices capable of receiving coded satellite signals without due authorization, or those devices that can be modified to do so.

Internet Key Sharing (IKS)

IKS, also known as CW sharing, is a fraud technique that allows a group of users to share an official smart card in order to be able to see encrypted signals without paying subscriptions. There are different ways to share official smart cards with other users, with Internet sharing currently being the most common. This requires connecting the illegal device to a remote Internet server. Illegal software in the device allows it to communicate with the smart card located in the remote server and obtain the required CWs to be able to access encrypted audio and video content.

This process is represented in Figure 3 and consists in the following five steps:

1. The ECM containing the encrypted CW is broadcast by the satellite and received by the illegal device.

2. Since the illegal device does not have the internal ability to decode the ECM, it sends the ECM to a remote IKS server through an Internet connection.

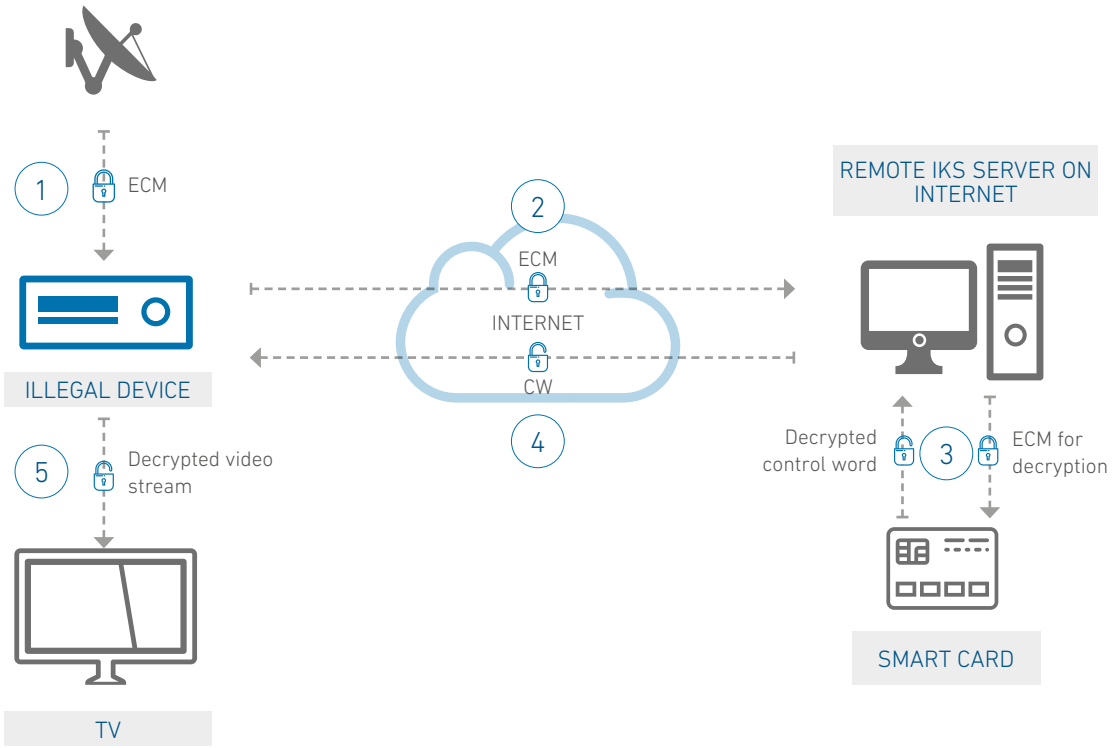
3. The IKS server receives the ECM and forwards it to the peripheral reader connected to the official smart card. This reader contains the official smart card and is able to decrypt the messages sent by the IKS server. The figure presents the case where the ECM is sent to the smart card and the decoded CWs are returned to the server.

4. The server then sends the decoded CWs to the illegal device.

5. Finally, the illegal device uses the CWs to decrypt the content of the subscription satellite television signal and shows it on the TV screen.

4 This chapter was prepared based on information provided by Nagra.

Figure 3: Architecture of an IKS system to commit fraud.

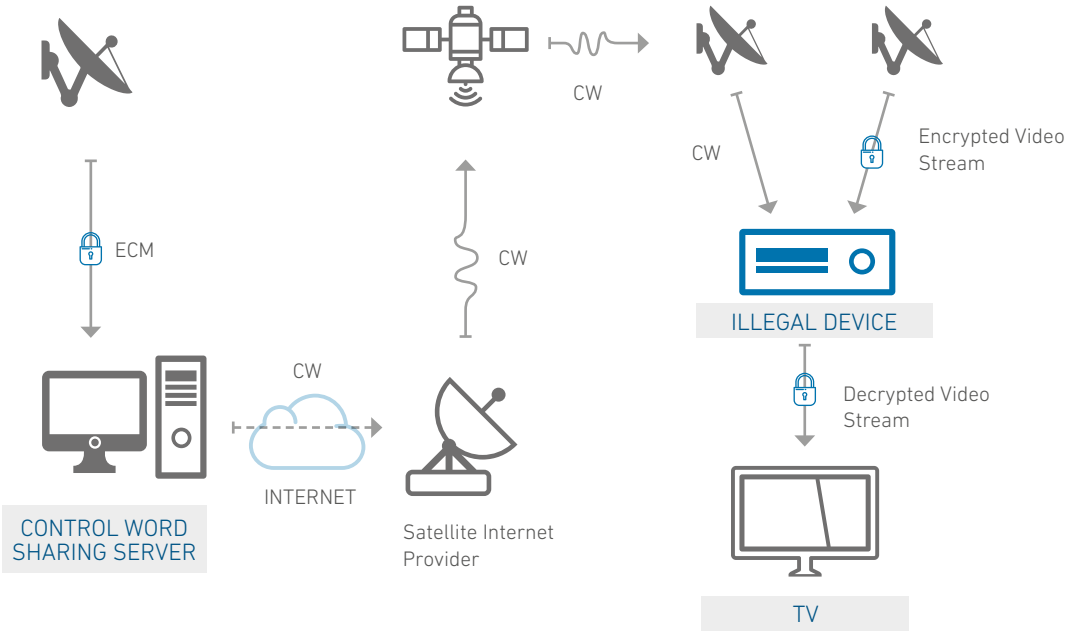


Satellite Key Sharing (SKS)

SKS, also known as Data Sharing via Satellite, is a fraud technique that allows users to simultaneously share the rights of a smart card with another group of users. It is done by sharing CWs using an IP (Internet Protocol) address via satellite connections (e.g. Internet satellite connections). CWs are continuously sent to the IP address. Then the Internet Service Provider (ISP) transmits the content sent to this IP address by means of the satellite. The equipment used to receive the SKS signals only needs to receive the packages containing the CWs in order to decrypt, in a fraudulent manner, the television signals in question (Figure 4).

The SKS method has several advantages for operators that commit fraud. Unlike the IKS architecture, the server load with the CWs does not depend on the number of users connected. In addition, the recipient is not relevant, since the SKS equipment team can get the CWs from any data packet sent by the satellite, according to the equipment's configuration. Likewise, it is not possible to identify the IP address of the end users using SKS because they do not need to connect to the Internet. Finally, it is very easy to access the CWs. End users do not need to access the Internet to connect to the SKS server; they only need to be located in the coverage area of the satellite that transmits the CWs.

Figure 4: Architecture of an SKS system to commit fraud.



Attributes to be validated to identify illegal devices[5]

Preliminarily, it should be noted that the ability to decode encrypted signals depends directly on the *software* that runs on each device. Thus, in practice, the availability of *illegal software* for a device, as well as the latter's ability to run said *software*, are the key factors to determine to which category a given receiver belongs.

Most of the time, *illegal software* does not come pre-installed on the equipment; the users must download these programs and install them. This is why the manufacturers of illegal devices tend to argue that they not have any relationship with any of the writers of *illegal software*, so, in their view, their devices are *legal*.

However, not only the existence of said *software* is of interest to the manufacturers of *illegal devices*, users have to find it and easily download it into their devices. This interaction is what allows this fraudulent system to work. Therefore, in practice, it is possible to identify *illegal device* models, as they are precisely those for which *illegal software* is readily available, being designed with the required *hardware* and interfaces to make this process smooth. It is useful to point out that each *illegal device* model needs its own version of the *software*, so the development of *illegal software* demands deep knowledge of the technical specifications of the corresponding device.

5 When *illegal* is mentioned within the framework of this document, it must be interpreted as *use for unauthorized purposes.*

Chapter 3

Measures taken by the Member States of CITEL

23

This chapter presents the different measures adopted by the States Members of CITEL to combat fraud related to the reception of subscription television signals by means of unauthorized satellite television receivers.

The main source of information used to develop this chapter are the responses to the survey included in Resolution PCC.I/RES. 242 (XXVI-15)[6] and the report related to Recommendation PCC.II/REC. 45 (XXV-15). Ten (10) Member States had answered the survey to March 2016, of which nine (9) (90%) mention that, in their countries, there are regulatory measures to combat the importation, marketing, and/or use of devices capable of receiving satellite television signals without due authorization, or which can be modified to do so.

A country, Paraguay, responded that it has no regulatory measures; however, it is in the process of implementing some form of regulations.

6 The survey is attached as Annex 1.

Table 1. Member States of CITEL that adopted measures* to combat fraud in the reception of subscription-based satellite TV signals.

COUNTRY	MEASURES TO COMBAT FRAUD	DESCRIPTION OF THE MEASURE
BRAZIL	Law 12485 Res. 242/2000	It prohibits the importation, sale or advertising of devices that allow the piracy of paid TV signals. Certification of devices capable of receiving satellite television.
BOLIVIA	Supreme Decrees 1391 of 2012, and 572 of 2010 Bi-Ministerial Resolution 007 of 2014 ATT DJ RA TL LP 1833/2014	The Supreme Decrees No. 1391 of 2012 and No. 572 of 2010, together with Bi-Ministerial Resolution No. 007 of 2014, updated the schedule of goods subject to prior authorization and/or certification, thus: "*...for the importation and entry of telecommunications equipment in general, as well as devices and antennas used in the satellite reception, suppliers or sellers must request their Prior Authorization or Certificate to the ATT, in accordance with applicable regulations*." According to the aforementioned regulations, the Authority for the Regulation and Control of Telecommunications and Transport (ATT) issued Regulatory Administrative Resolution 1833 in 2014, which approved the *Guidelines* to grant either Prior Authorization for Importation and/or Certificate for the Customs Clearance of telecommunications devices. The same Resolution contains the Requirements for the Prior Authorization for devices capable of receiving satellite television (decoders and dongles). The regulations dictate that "*... the application must be submitted by the legal representative of an operator that has the operating permit to be able to provide the service of signal distribution, or by broadcasting operators that have signal on a space station (satellite) or by service providers that provide added value in the distribution of signals that have signal on a space station (satellite).*" In case of imports made by intermediary companies, they must attach to their application a Certificate by an operator and/or service provider that is legally authorized by the ATT.
COLOMBIA	Law 182 of 1995 Law 599 of 2000 Resolution ANTV 433 of 2013	In articles 24 and 25, Law 182 of 1995 stipulates that any natural or legal person that undertakes the reception and distribution of encoded signals without authorization shall be deemed engaged in and the provider of an illegal clandestine service, and, as such, shall be subject to the sanctions stated in the law. Law 599 of 2000 instituted that "any clandestine mechanism or alteration of control systems or counters used to obtain (...) telecommunications signals to the detriment of a third party, shall be punishable by a prison term of sixteen (16) to seventy-two (72) months, and a fine of 1.33 to 150 minimum monthly wages, as applicable." Article 24 of Resolution ANTV 433 of 2013 states that License Holders to the Community Television Service are prohibited from "using any decoding, reception or distribution technical mechanism that allows receiving and/or distributing television signals without the prior and express authorization of the owner/holder of the copyright and related rights."

COUNTRY	MEASURES TO COMBAT FRAUD	DESCRIPTION OF THE MEASURE
ECUADOR	Resolution No. 93 of November 19, 2012, by the Foreign Trade Committee of Ecuador.	The importation of decoders and satellite receivers classified under Subheading 8528.71.00.10 (Decoders: FTA satellite receivers) through Correos del Ecuador (Ecuador's state-owned postal service) or Courier services, or by means of natural persons that enter the country by international airports, borders, or maritime ports. Ecuador's National Customs Service shall order the reshipment of these goods as soon as they are seized. Imports through a license issued by the Agency for Regulation and Control of Telecommunications.
UNITED STATES	USC 18 USC 47 USC 17	It is hereby forbidden: To intercept "electronic communications" (satellite signals). To mail or transport, through interstate or international boundaries for the purpose of sale, any electronic, mechanical or other device, when there is knowledge or reason to infer that the design of this device may be useful to intercept wireless, sound or electronic communications. To build, assemble, own or sell any electronic, mechanical or other device, when there is knowledge or reason to infer that the design of this device may be useful to intercept wireless, sound or electronic communications, and that such device or any of its components have been or will be sent by mail or transported through interstate or international boundaries for the purpose of sale. To publicity advertise devices that allow signal theft in newspapers, magazines, or other publications. To use the "device" in violation of 18 USC 2511 or 2512. The construction, assembly, modification, import, export, sale or distribution of an electronic, mechanical or other device that allows unauthorized decryption of direct-to-home satellite services. To receive or help others receive "radio signals" (satellite TV) without authorization. To receive or help others receive "radio signals" (satellite TV) without authorization in order to obtain a commercial advantage or private gain. The circumvention of copyright protection systems.
PANAMA	Resolution AN No.5047-RTV	The National Public Services Authority issues guidelines related to the importation, distribution, installation, marketing, acquisition and use of receiving devices that allow access to the content of "direct to home" satellite television (DTH equipment), in order to warn about their administrative consequences and penalties from bad practices in the promotion and installation of such devices. Likewise, the Criminal Code of the Republic of Panama establishes fines and even prison terms for the illegal use of telecommunications signals, including satellite signals, depending on the classification of the felony or crime.

COUNTRY	MEASURES TO COMBAT FRAUD	DESCRIPTION OF THE MEASURE
PERU	Law No. 29316 Supreme Decree No. 013-93 Supreme Decree No. 001-2006	Law 29316 prohibits the manufacturing, assembly, importation, export, sale, or rental of a device or system, tangible or intangible, whose main function is to help decode a coded satellite signal that carries broadcast programs without the authorization of the legal Distributor of said signal, establishing penalties for those parties that carry out such actions. Supreme Decree 013-93 classifies as a serious felony the importation, manufacturing, distribution and sale of equipment, terminals or devices that do not have a certificate of approval or validation, deeming a very serious felony the unauthorized interception or interference of telecommunications services that are not free to air for the general public. Supreme Decree 001-2006 states that felonies related to the validation of telecommunications equipment and devices are indicated in the Law, its General Regulations, and in the field of broadcast services by the Law of Radio and Television and its Regulations. Any such devices must be submitted for their inspection, classification, and punishment if applicable.
URUGUAY	Decree 276/12	It forbids the manufacture, importation, sale, rental, and circulation of certain brands of satellite receivers. No satellite receivers can enter the country without the authorization of the Regulatory Unit of Communications Services.

* Information to March 2016.
Source: Questionnaire about Resolution PCC.I/RES. 242 (XXVI-15), "Compilation Report on the Measures and Provisions Adopted to Prevent the Use of Unauthorized Receiver Devices for Subscription Satellite Television", document 4086r1, XXVII Meeting of PCC.II.

Table 2: Countries that are analyzing measures* to combat fraud in the reception of subscription-based satellite TV signals.

COUNTRY	IS IT ANALYZING MEASURES? WHICH?
COLOMBIA	In addition to the measures detailed in the previous Table, and for the implementation of the Social DTH Project, document 3815 of 2014 by the National Council of Economic and Social Policy (CONPES) calls to *strengthen* the accompaniment provided by the Prosecutor General of the country to the National Tax and Customs Authority (DIAN), the national police, and the National Television Authority (ANTV) in their actions to combat the smuggling and illegal use of receivers to capture television signals and the unauthorized distribution of television signals. It also urges for collaboration between the aforementioned authorities to assess the need for additional customs requirements in order to control the entry of smuggled equipment and prevent the operation of those that do not meet minimum technical specifications.
PARAGUAY	Validation of receivers. Agreement with customs to prevent the importation of non-approved devices. Inspections to shops that sell these receivers.

* Information to March 2016.
Source: Questionnaire about Resolution PCC.I/RES. 242 (XXVI-15).

Chapter 4

International Best Practices

This chapter presents the experiences and measures adopted by countries that are not members of CITEL to combat fraud related to the reception of subscription television signals by means of unauthorized satellite television receivers. Given their relevance, we present the measures adopted at the level of the European Union and their transposition in the main Member States. This initiative represents a valuable experience for the regional harmonization of legal standards and best practices to avoid fraudulent conduct by means of the unauthorized reception of CAS-protected signals.

In 1998, European Union authorities adopted Directive 98/84/CE to harmonize "the provisions of Member States related to measures against illegal devices that allow unauthorized access to protected services."[7]

According to Directive 98/84/CE, protected services include, among others, television services, "provided they are provided in exchange for remuneration and on the basis of conditional access."[8] In addition, the standard in question defines illegal devices as "any device or computer program designed or adapted to make possible access to a protected service in an intelligible fashion, without the authorization of the service provider."[9] As you can see, the characteristics of illegal devices described in this document satisfy the criteria stipulated down in the aforementioned European Union Directive.

In this context, Directive 98/84/CE required Member States to prohibit the following activities, defined as illegal:

a. "the manufacture, importation, distribution, sale, rental or possession for commercial purposes of illegal devices;

b. the installation, maintenance or replacement for commercial purposes of an illegal device;

c. the use of commercial communications to promote illegal devices." [10]

In view of the obligation to transpose this EU regulation[11], several Member States have adopted legal, regulatory and administrative provisions against illegal devices. The following table shows a list of countries and their respective regulations concerning this matter. All these countries have defined the aforementioned activities as illegal.

---

7 See Article 1 of DIRECTIVE 98/84/CE OF THE EUROPEAN PARLIAMENT AND COUNCIL dated November 20, 1998, relative to the legal protection of conditional access systems or those based on said access, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:320:0054:0057:ES:PDF

8 Id., Art. 2.

9 Id., Art. 2(e).

10 Id., Art. 4.

11 Id., Art. 6(1).

Table 3: Transposition of Directive 98/84/CE in the main Member States.

COUNTRY	REGULATION
GERMANY	Forbidden: (1) The manufacture, importation and commercial dissemination of devices designed or adapted for unauthorized use of a conditional access service; (2) The possession, installation and maintenance for commercial purposes of devices designed or adapted for unauthorized use of a conditional access service; (3) The promotion of devices designed or adapted for unauthorized use of a conditional access service. March 19, 2002[12]
SPAIN:	1. Punishable by imprisonment from six months to two years and a fine of six to 24 months - Anyone who , without the consent of the service provider and for commercial purposes, were to provide intelligible access to a sound or television broadcasting service, interactive services provided remotely by electronic means, or supply conditional access to the aforementioned services, considered an independent service by means of: 1.1 The manufacture, importation, distribution, availability through electronic means, sale, rental, or possession of any device or computer program that is not authorized in another Member State of the European Union, or designed or adapted to make such access possible. 1.2 The installation, maintenance or replacement of the devices or computer programs mentioned in paragraph 1.1. 2. The same punishment shall be handed to those who, with the aim of profit, alter or duplicate the identification number of telecommunications devices, or those who sell computers that have already undergone fraudulent modifications. 3. Those who, without the aim of profit, facilitate the access described in paragraph 1.1 to third parties, or by means of a public communication, commercial or not, to supply information to several people on how to get unauthorized access to a service or the use of a device or program included in that same paragraph 1.1, inciting to achieve them. This shall be punishable by the fine stipulated therein. 4. Those that use devices or programs that allow unauthorized access to conditional access services or telecommunications equipment shall be punishable pursuant to Article 255 of this Code, regardless of the amount of the fraud. Article 286 of Organic Law 10/1995[13]
FRANCE	Punishable by two years' imprisonment and a fine of 30,000 Euros - The manufacture, importation for sale or rental, offer for sale, possession for sale or installation of equipment, materials, devices or instruments with fraudulent design, in whole or in part, in order to capture broadcast programs when said programs are limited to a specific audience in exchange for a fee paid to the service operator. Law No. 86-1067 of September 30, 1986, relative to freedom of communication, with modifications - Article 79-1[14]

12 See http://ec.europa.eu/internal_market/media/docs/elecpay/natimpl/germany/germany1_de.pdf
13 See http://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf
14 See http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068930#LEGIARTI000006420700

COUNTRY	REGULATION
ITALY	The following activities are forbidden: (a) The manufacture, importation, distribution, sale, rental or possession for commercial purposes of any illegal device; (b) the installation, maintenance or replacement for commercial purposes of an illegal device; (c) the use of any means of commercial communication to promote the distribution and use of illegal devices. Illegal device: Any device or software designed or adapted to make possible access to a protected service in an intelligible fashion, without the authorization of the service provider. Legislative Decree 15.11.2000, No. 373[15]
PORTUGAL	The following activities are forbidden: (a) The manufacture, importation, distribution, sale, rental or possession for commercial purposes of illegal devices; (b) the installation, maintenance or replacement for commercial purposes of an illegal device; (c) the use of commercial communications to promote illegal devices. Illegal device: Any device or software designed or adapted to make possible access to a protected service in an intelligible fashion, without the authorization of the service provider. Executive Decree No. 287/2001[16]
UNITED KINGDOM	A person commits a felony if he/she: (a) manufactures, imports, distributes, sells, or rents unauthorized decoders, or offers or displays them for sale or rental; (b) has in his/her possession unauthorized decoders for commercial purposes; (c) installs, services or replaces unauthorized decoders for commercial purposes; (d) advertises unauthorized decoders for sale or rental, or in another way promotes unauthorized decoders by means of commercial communications. Statutory Instrument 2000 Nr. 1175 - Conditional Access (Unauthorized Decoders) Regulations 2000[17]

Source: Regulations in each country.

15 See http://ec.europa.eu/internal_market/media/docs/elecpay/natimpl/italy/italy-legalprotection_en.pdf
16 See http://ec.europa.eu/internal_market/media/docs/elecpay/natimpl/portugal/portugal1_pt.pdf
17 See http://ec.europa.eu/internal_market/media/docs/elecpay/natimpl/uk/uk1_en.htm

Chapter 5

Recommendations

This chapter presents a series of recommendations to efficiently combat fraud in the reception of subscription-based satellite television signals through illegal devices: those that have the ability to decrypt or facilitate the decryption of subscription-based satellite TV signals without proper authorization, or which can be modified for this purpose.

The objective is to adopt and apply recommendations on best practices at the national level in the Member States of the OAS/CITEL so that fraud prevention policies are congruent and harmonized at the regional level.

The following are different aspects that should be considered for adopting by the Member States of CITEL/OAS to better combat fraud in the reception of subscription-based satellite television signals through illegal devices.

Recommendations

» To develop a legal framework to fight against the manufacture, importation, distribution, rental, marketing, promotion, installation, circulation, and/or use of illegal devices.

» To develop a legal framework to punish the circumvention, evasion, disabling, and/or suppression of the technological security measures set up by the holders of subscription satellite TV signals and/or the holders of the contents of such signals.

» To focus more efforts on the control of those stages prior to the use of illegal devices by end users.

» Establish, as requisite for the entry of FTA devices without the ability to decrypt signals from subscription satellite TV systems or that could be modified for this purpose, a framework of suitable controls that ensures their correct harmonization to restrict the import, distribution, sale, and circulation of these devices. For the purposes of control, and in view of the complexity of the technology involved, the relevant authorities may require the industry to cooperate in controlling the entry of the FTA devices in question, providing an independent specialized technical team to which the authorities can recur in order to determine such harmonization.

» To establish provisions to ensure that decoder devices with the ability to decrypt encoded signals may only be imported by authorized pay television operators whose license enables them to carry out such imports.

» Based to the attributes described in this report, to define the procedures that allow the identification of illegal devices.

» To develop a monitoring system that allows the traceability of satellite television receivers.

» To develop a system through which complaints can be channeled when fraudulent practices related to the manufacture, importation, rental, marketing, distribution, promotion, installation, circulation, and/or use of illegal devices are verified.

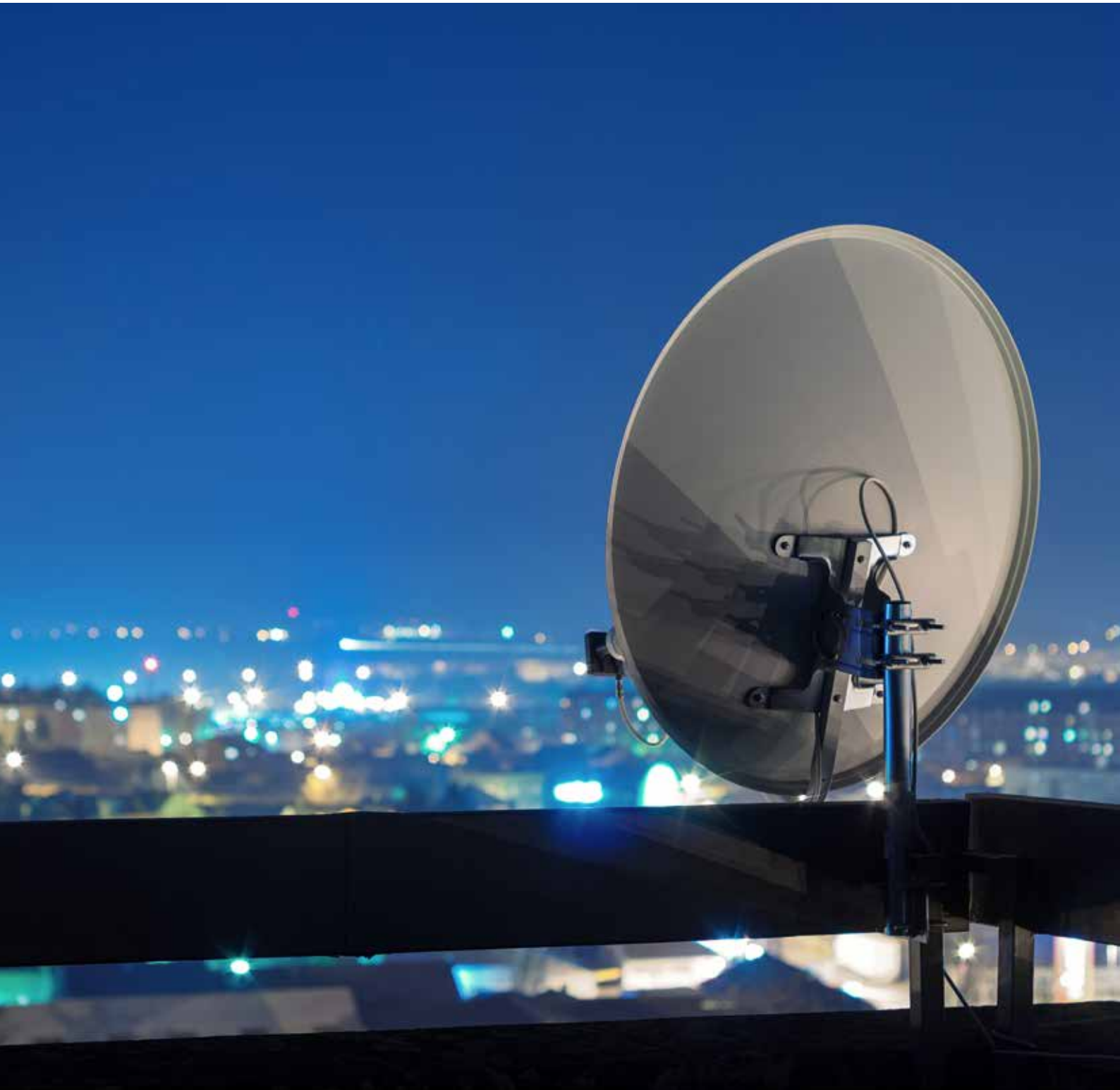
» To combat any commercial communications

by any means that deal in the promotion of illicit devices.

» To establish a system of appropriate penalties when detecting non-compliance within the legal framework that is already applicable or to be implemented.

» To improve the performance and coordination of different State agencies and private operators involved in the aforementioned activities.

» To promote the harmonization of policies related to the control of this type of fraud among the Member States of CITEL.



Annex

Glossary

CAS	Conditional Access System
CW	Control Word
DTH	Direct-To-Home
ECM	Entitlement Control Messages
FTA	Free-To-Air
IKS	Internet Key Sharing
IP	Internet Protocol
ISP	Internet Service Provider
SKS	Satellite Key Sharing
STB	Set Top Box
VPN	Virtual Private Network

CITEL

Inter-American Telecommunication Commission

Permanent Consultative Committee I: Telecommunications/Information and Communication Technologies (PCC.I)

1889 F St. NW

Washington, DC, Unites States of America

www.citel.oas.org

Executive Secretariat of CITEL
Phone: +1 202 370 4713
Fax: +1 202 458 6854

E-mail: citel@oas.org

June, 2017

OAS|CITEL | ALIANZA
CONTRA LA PIRATERÍA DE TELEVISIÓN PAGA